NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN ANALYSIS OF CHINA'S INFORMATION TECHNOLOGY STRATEGIES AND THEIR IMPLICATION FOR US NATIONAL SECURITY REPUBLIC OF CHINA

by

Wen-Hsiang Tsai

June 2006

Thesis Advisor:	Karl D. Pfeiffer
Second Reader:	Glen Cook

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: An Analysis of China's Information Technology Strategies and their Implication for US National Security.			**5. FUNDING NUMBERS**
6. AUTHOR(S) Wen-Hsiang Tsai			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

In the past decades, China's military modernization and economy fast development has increasingly attracted international attention, especially the United States. In addition, the PLA has begun to study the revolution in the military affairs (RMA) by focusing on asymmetric warfare capabilities under high-tech conditions. China definitely believes that asymmetric warfare operations have the advantage of creating a more smart attack style to avoid directly facing U.S. powerful military strength. In summary, asymmetric warfare operations are considered by the PLA as a kind of warfare that combined both the thinking of China's classic military strategist Sun Tzu *"using the inferior to defeat the superior"* and the demand of the modern information technology such as IW applications.

In face of China's development of asymmetric warfare capabilities, the United States must deeply think about how to deal with the threat from China's asymmetric warfare operations, which is gradually becoming the superpower in the world.

14. SUBJECT TERMS United States, People's Republic of China, Republic of China ,Taiwan, Taiwan Strait, PLA, Military Moderation, Information Warfare, Asymmetric Warfare			**15. NUMBER OF PAGES** 107
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN ANALYSIS OF CHINA'S INFORMATION TECHNOLOGY STRATEGIES AND THEIR IMPLICATION FOR US NATIONAL SECURITY

Wen-Hsiang Tsai
Captain, Army, Taiwan, Republic of China
B.S., Chung-Cheng Institute of Technology, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2006

Author: Wen-Hsiang Tsai

Approved by: Karl D. Pfeiffer
Thesis Advisor

Glen Cook
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In the past decades, China's military modernization and rapidly developing economy have increasingly attracted international attention, especially the United States. In addition, the PLA has begun to study asymmetric warfare capabilities under high-tech conditions. China definitely believes that asymmetric warfare operations have the advantage of creating a smarter attack style to avoid directly facing U.S. military strength. In summary, asymmetric warfare operations are considered by the PLA as a kind of warfare that combined both the thinking of China's classic military strategist Sun Tzu *"using the inferior to defeat the superior"* and the demand of the modern information technology such as IW.

In face of China's development of asymmetric warfare capabilities, the United States must deeply think about how to deal with the threat from China's asymmetric warfare operations, which is gradually becoming the superpower in the world.

.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my sincere thank to my thesis advisor Karl D. Pfeiffer, who inspired me to pursue the subject of this thesis and second reader Mr. Clen Cook who give me a lot of assistant for study in the NPS. Their overwhelming support, guidance and untiring patience were the key factor for this thesis successful completion.

In addition, I would like to express my deepest thanks to my lovely wife, Sun, Miao-Fen. Her patience, understanding and ability to maintain a comfortable home during this difficult time make me get through the thesis process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

China is the world's most populous country and one of its largest. China's territory covers 9.3 million square kilometers, nearly 10 percent of the Earth's surface, stretching almost 5,000 kilometers (3,100 miles) from east to west and 5,500 kilometers (3,410 miles) from north to south. China's population, estimated at about 1.3 billion people, continues to grow at 0.7 percent per year. Its population represents almost 20 percent of the world's 6.3 billion people.

In 1912, China became a republic under the leadership of Sun Yat-sen, who used a Western-oriented ideology to unify the elements of the declining Chinese empire. That transition to a more Western political thought, however, still carried a certain Sino-imperial character. Following Sun Yat-sen's death in 1925, his brother-in-law, Chiang Kia-shek, maneuvered for control of the Chinese Nationalist Party (KMT) and then dominated Chinese politics until the end of the Second World War. After Japan was defeated, a civil war erupted in China, which lasted until 1949, when the Chinese Communist Party (CCP) won control of the mainland and the Chinese Nationalist Party (KMT) withdrew to the island of Taiwan.

A year later, with the outbreak of the Korean War and the threat of a possible Chinese attack on Taiwan, President Harry S. Truman ordered the 7th Fleet into the Taiwan Strait. It was the United States' first intervention in the conflict between the island and mainland China. The United States considered Taiwan as a buffer against communist expansion in Asia and therefore provided the island with financial and military support.

Mao Ze-dong (Mao Tse-tung), one of the great theorists of Marxist communism and one of the founding fathers of the Chinese Communist Party (1921), was elected chairman in 1931. From 1966 to 1976, Mao imposed a catastrophic so-called Cultural Revolution on the Chinese people, but China made little economic progress. Mao Zedong's death in 1976 was followed by a two-year struggle for power, from which Deng Xiaoping (Teng Hsiao-p'ing) emerged as leader of the People's Republic of China

(PRC). Deng discarded many of Mao's policies and implemented economic reform, shifting from an unprofitable state-owned-enterprise (SOE) to economic policies that were more attractive to foreign investment, established special economic zones, and allowed a wide variety of privately owned enterprises and small-size light industries in service.

China's economic reform differed from that of contemporary Russia, however, which also included political reform. While China's economy doubled in size from 1989 to 1999, there were few political alterations but Russia has struggled in its effort to build a democratic political system to replace original communism government systems and make little progress on market economy.

In 1995, the Chinese administration adopted a fifteen-year national development program, with a huge budget, to run from 1995 to 2010 [4]. There were six key components:

1. Improving freight shippers' security and passengers' safety by implementing modern technology to satisfy customers' high expectations.
2. Increasing the speed of passenger trains to 140 or 160 km/hour (approximately 87 to 99 miles/hour) on the Beijing- Shanghai, Beijing-Harbin, and Beijing-Guangzhou trunk lines. Also, increasing the speed of freight service.
3. Introducing a computer network system to process seat reservations and raising the comfort standards, by adding high-quality, double-deck coaches and air-conditioning for long-distance tourist trains.
4. Developing internet technology and using computers for operational management.
5. Upgrading the traditional long-haul lines and other old trunk routes with new optical-fiber and wireless communications systems.
6. Raising the standards for construction and engineering work through modern technology.

Today, the People's Republic of China continues to accelerate the pace of its economic reform: it has the world's second-largest economy, second only to the United States [4]. Though communism may be fading in China, Mao Zedong's nationalism and China's ambitions for Asia and the world remain strong.

B. MOTIVATION

Since its establishment as the People's Republic of China in 1949, a relatively short period of time, China has developed comparatively complete systems of defense, technology, and industry. In the field of sophisticated technology, its successful development of missiles, atomic bombs, and man-made satellites makes China one of the few countries in the world with nuclear weapons and space technology. In the field of conventional equipment, China made a fundamental change from copying others' designs to independent production. Militarily, these accomplishments allowed it to transform its military from a simple ground force into an integrated armed service comprising army, navy, air, and Second Artillery (strategic nuclear) forces. In addition, China invested in long-distance cruise missiles and submarines to challenge U.S. naval power in the Pacific.

Beginning in the 1980s, the People's Liberation Army (PLA) also adopted military modernization programs intended to update its obsolete post–Korean War equipment with newer weapons. The military began purchasing high-tech weapons from foreign sources to modernize its navy, air force, and missile infrastructure. These programs have significant improved its overall military capabilities.

Expense / Item / Year	Personnel Expenses	Maintenance of Activities	Costs for Equipment	Total
1998	322.7	298.0	314.0	934.7
1999	348.6	380.3	347.8	1076.7
2000	405.5	418.1	389.3	1212.9

Table 1. Composition of China's Defense Expenditures in 1998, 1999 and 2000 (Unit: RMB billion Yuan) (After: http://www.fas.org/nuke/guide/china/doctrine/cnd0010/china-001016wp5.htm, Accessed August 8, 2005).

Table 1 shows China's 1998–2000 defense expenditures, divided into three categories: personnel expenses (salary, food, and clothing), maintenance cost of activities (construction and maintenance of military facilities, personnel training, annual military

exercises), and equipment costs (advanced weapons research and experimentation, weapons procurement from foreign countries, self-manufacture, maintenance, transportation, and storage). The defense budget for those years is estimated at as much as $90 billion. Moreover, China's defense budget continues to increase in keeping with the rapid growth of its economy, making China the world's third-largest weapons buyer (Russia is second to the United States) and the biggest buyer in Asia.

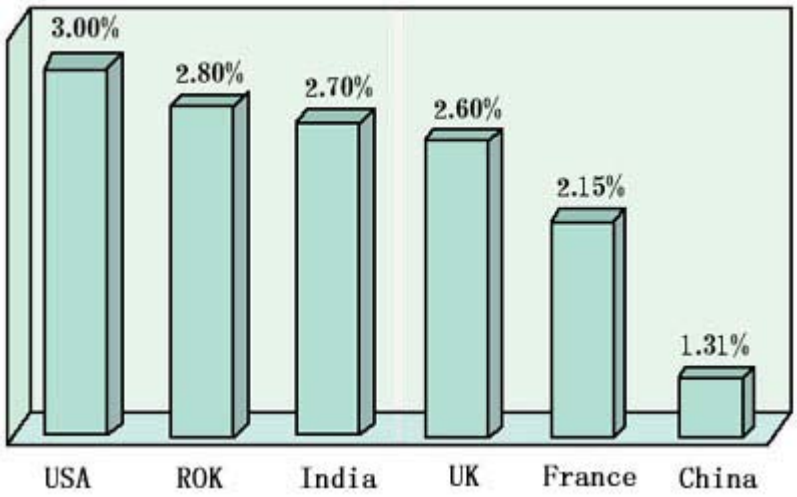

Figure 1. The Percentage of Defense Expenditure in the GDP of Some Countries in 1999. (From: http://www.fas.org/nuke/guide/china/doctrine/cnd0010/china-001016wp5.htm, Accessed September 29, 2005).

We know that China is investing much of its capital in its advanced weapons system, but its defense budget per capita is still smaller than that of the United States (See Figure 1, China 1.31 % less than U.S. 3.00 %). Also its high technology level is a great distance behind that of the United States.

In keeping with the principles of China's classic military strategist, Sun Tzu, two senior PLA colonels propose "using the inferior to defeat the superior" and "winning the war without bloodshed." In their book, *Unrestricted Warfare***,** Qiao Liang and Wang Xiangsui propose a series of asymmetric strategies for securing China's dominance as a global power [2]. *Unrestricted Warfare* proposes that China is unlikely to challenge the United States with conventional kinetic methods, so it suggests an offensive style of warfare that surpasses all conventional boundaries, ethics, and concepts of war to topple

American hegemony. In this book, the two PLA authors discuss twenty-four different "military," "transmilitary," and "nonmilitary" strategies.

TYPE	EXPLANATION
Terrorist warfare	aircraft suicide attacks causing public panic
Financial warfare	breaking down banking systems, stock markets, and monetary systems
Psychological warfare	spreading rumors to intimidate the enemy and break down the enemy's will
Media warfare	manipulating what people see and hear in order to influence public opinion
Smuggling warfare	throwing markets into confusion and attacking the economic order
International law warfare	blocking enemy actions by using multinational organizations, for example, six-party talks
Resource warfare	seizing control of curial natural resources, such as China National Petroleum's purchase of Petrokazakhstan, which controlled vast oil reserves in the Central Asian republic of Kazakhstan
Network warfare	venturing out in secret and concealing one's identity in a type of warfare that is virtually impossible to guard against
Technological warfare	creating monopolies by setting standards independently
Cultural warfare	using its own influence to assimilate those with different views
Ecological warfare	creating man-made drought or other environmental disasters

Table 2. Type of Asymmetric Warfare

In modern warfare, all of these strategies could be combined and practiced for the single purpose of defeating an enemy without incurring significant loss of personnel or equipment. This thesis will analyze the information technology strategies of both the People's Republic of China and the People's Liberation Army. The thesis will focus on an analysis of the asymmetric strategies employed by the PRC to secure their dominant position in Asia and the world.

C. ORGANIZATION

Chapter II will give a brief history of the relationship between the ROC, the PRC, and the United States, especially with respect to the U.S. role in the Taiwan Strait.

Chapter III will discuss the traditional military capabilities of the PLA navy, air force, army, and SAC to clearly show China's integrated armed service capabilities.

Chapter IV will discuss how the People's Liberation Army has been influenced by modern Western military thought, especially focused on China's information warfare capability.

Chapter V will explain the key factors that might trigger the PRC to pursue asymmetric warfare strategies and capabilities.

Chapter VI will explore case studies of unrestricted warfare as practiced by the PRC against U.S. interests.

Chapter VII will provide a summary and recommendations for future research.

II. THE RELATIONSHIP BETWEEN THE REPUBLIC OF CHINA (ROC), THE PEOPLE'S REPUBLIC OF CHINA (PRC), AND THE UNITED STATES

A. INTRODUCTION

Recently, legislators from the pro-independence Taiwan Solidarity Union supported the Taiwanese people in sending emails to the famous U.S. Internet search engine, Google, protesting its description of Taiwan. Their goal was to make Google refer to Taiwan as an independent country. In response, in October 2005, Google made a crucial decision: to stop calling Taiwan a Chinese "province." Not surprisingly, Google's deletion of the words "a province of the People's Republic of China" from its map of Taiwan triggered a serious reaction from China. A Chinese official, Peng Keyu, told the Singtao Daily that China was angry and disappointed that Google had deleted the "correct" sentence from the top left corner of its Taiwan-map webpage. China continues to consider Taiwan part of its territory, though many Taiwanese today consider themselves citizens of an independent nation. Google spokeswoman Debbie Frost told the China news agency Xinhua that the event was just a normal update of their Web site's map pages, not an effort specifically to update the Taiwan page. However, in chat rooms around the country, many mainland Internet users are suggesting a boycott of Google's China service [61].

Taiwan and China share the same culture, language, and ancestry, but are divided both geographically, by the narrow Taiwan Strait, and politically into totally different government systems. Taiwan, on the east side of the Strait, has focused on democratic, human rights and economic and industrial development. As a result, Taiwan has become one of the most highly industrialized countries in Asia. Since the Chinese split into two countries, the United States has played a very important role in the Taiwan Strait. Sometimes it acts as a participant, sometimes as an observer. Before Taiwan left the U.N., the United States was Taiwan's closest and strongest ally; it helped Taiwan get through its darkest period of time.

In this chapter, we will review the complex relationship between Taiwan, China, and the United States. Our understanding of how these often adversarial relationships

have evolved will inform our subsequent discussion of the current asymmetric strategies of the People's Republic of China.

Figure 2. Map of China (From: Yahoo Education, http://education.yahoo.com/reference/factbook/ch/ map.html, Accessed September 11, 2005).

B. CHINESE CIVIL WAR (1946–1950)

During the Sino-Japanese War, part of World War II, the Soviet Union sent "seed" communists into China to develop a Chinese Communist Party. The war heightened China's rural poverty and made the Chinese people eager to pursue an ideal government. That and the consequences of the wartime destruction provided the Chinese Communist Party with a convenient laboratory for social and economic reform.

The Chinese Civil War from 1946 to 1950 was one of the many critical struggles of the twentieth century. Its results would determine China's subsequent history, especially its international affairs in East Asia, up to the present time. The civil war was a conflict between two ideological trends: democracy, represented by the Chinese Nationalist Party (KMT), and communism, represented by the Chinese Communist Party (CCP) [25]. During this period, though economic and political factors had little impact on

the progress and outcome of the war, the CCP transformed itself into an agrarian communist society to maximize support among the large peasant class in late-1940s Chinese society.

Because the Chinese government, the Chinese Nationalist Party (KMT) at the time, joined with the Western alliance during World War II, it received much of the benefit of U.S. wartime aid. After the war, the KMT, which controlled the more advanced provinces along the coast, was not only treated as the government of China and but was also given that formal position internationally. Mao's control was in the Chinese interior and to the north.

For a long time, the Chinese Communist Party could not match the Chinese Nationalist Party militarily — whether in troop training, equipment, or numbers. However, the Chinese Nationalist Party's economic mismanagement and corruption caused economic inflation throughout the country. In the meantime, the CCP continued to be dedicated to radical land reforms, which were very popular with the Chinese people.

After Japan's surrender in Manchuria in 1945, the Soviet Union gave the Chinese Communist Party considerable quantities of surrendered Japanese military equipment and weapons. This gave the CCP an opportunity, which they used to their advantage, to enhance their overall military capability for the upcoming civil war. At the same time, after years of struggle with the Japanese, the KMT government's reserve of military power, supplies, and material resources, as well as the troops' morale and the people's support, were all seriously reduced.

The Nationalist Party's greatest mistake was its failure to make use of certain initial advantages. First, the KMT implemented reprisals against those who had remained under Japanese rule, which increased the mistrust of the people and some members of the government. Some original party members became less supportive of the KMT and, eventually, became members of the Chinese Communist Party. Second, the Party failed to explore both domestic and international alliances, a failure that left them isolated, without allies.

By comparison, the strength of the CCP lay in its exploitation of the KMT's weaknesses and its use of asymmetric strategies against that better-funded and better-

equipped opponent. One example of this was the propaganda war which successfully stigmatized the KMT as an enemy of all groups of Chinese, poor and rich, peasant and bourgeois. In addition, the CCP's alliance with the Soviet Union provided it with international legitimacy and military assistance.

By mid-March 1948, the KMT held only fragments of the mainland; and then its forces collapsed. Mao's troops drove south across the Yangtze, capturing Shanghai and forcing the remaining KMT forces into the west. In 1949, the KMT withdrew to Taiwan, where Chiang Kai-shek established his government.

At the time, President Truman made his position clear: "The United States government will not pursue a course which will lead to involvement in the civil war in China" [2]. Nonetheless, the United States aided the KMT with massive economic loans, but no military support. However, realizing that the U.S. efforts fell far short of a large-scale armed intervention and that they could not stop the war, the United States dispatched General George Marshall to negotiate peace between the KMT and the CCP and prevent a widespread civil war. Finally, through the mediatory influence of the United States, a military truce was arranged in January 1946, but battles between Nationalists and Communists soon resumed. By that time, U.S. attention had become more focused on Europe than on Asia. China had no strategic importance to the United States and was not perceived as a threat to the United States in the future. Although the CCP takeover of China was not desirable, for the United States it was a tolerable outcome.

Figure 3. Map of Korea (From: Yahoo Travel, http://travel.yahoo.com/p-travelguide-577920map_of_korea_southi;_ylc=X3oDMTE3N2phcW1vBF9TAzI3NjY2NzkEX3MDOTY5NTUzMjUEc2VjA3NyBHNsawN0aXRsZQ, Accessed September 11, 2005).

C. THE KOREAN WAR (1950–1953)

Korea had long been an independent kingdom under a Chinese suzerainty [10] when Japan, following its victory in the Russo–Japan War, first occupied Korea, and then, in 1910, formally annexed the entire peninsula. In 1945, after Japan was defeated in World War II, Korea was divided at the 38th Parallel into two zones of occupation, north and south, a Soviet zone and a U.S. zone, respectively.

By 1948, South Korea had become the Republic of Korea, and North Korea, the People's Democratic Republic of Korea. Eventually, when the Chinese communist revolution achieved a nationwide victory, Kim IL Sung, the leader of North Korea, planned to unify the entire Korean peninsula through a revolutionary war. From summer 1949 to spring 1950, the Chinese and Korean communist leaders had a series of

discussions that resulted in the CCP sending between 50,000 and 70,000 ethnic Korean PLA soldiers—the core of the North Korean Army offensive—with their weapons, back to Korea. In doing so, the CCP gave Kim the green light to attack the South, and, in June 1950, North Korea invaded South Korea. Both China and the Soviet Union supported the invasion, though China did not commit troops until General Douglas MacArthur pressed too close to the 38th parallel. Korea became an issue for the United States because of the fall of the KMT in mainland China. That is, the retreat of Chiang Kai-shek to Taiwan drew an ideological line in the sand for the U.S. administration, so the invasion of North Korea across the 38th parallel in June 1950 demanded a military response.

After months of heavy fighting, the center of the conflict was once again the 38th parallel, where it remained for the rest of the war. Due to public criticism of the United States's Korean War policy, President Truman, on the recommendation of the Joint Chiefs of Staff, removed MacArthur and, in April 1951, installed General Matthew B. Ridgway as commander in chief. General Ridgway began truce negotiations with North Korea and China, and, on 27 July 1953, the Korean War ended and an armistice agreement was signed[9].

China remained North Korea's main ally throughout the Cold War period. It was only massive Chinese military interventions that saved the North Korean regime from an imminent collapse. Since the end of the Cold War and the disintegration of the Soviet Union, China has become the sole big power from which North Korea receives substantial material support. Now North Korea has said that it intends to develop its own nuclear force. China transferred a nuclear weapons capability to North Korea as part of its strategy against the United States, which was threatening to use all means to stop that from happening.

How the crisis situation on the Korean peninsula will develop, be controlled, and be resolved depends largely on what China can and will do. China deliberately adopted an asymmetric warfare strategy that included North Korea's economic dependence on China, so that North Korea would serve a strategic buffer on China's northeastern border. China needs a stable and peaceful environment in East Asia so that it can continue its

economic and military modernization and extend its influence beyond the Asian borders [39].

The outbreak of the Korea War was a shock to the United States and intensified the hostilities between the communist and noncommunist camps in the accelerating East–West arms race. Moreover, until October 1958, a large number of China's volunteer troops remained in North Korea, and China began to play an increasingly important role in Korean affairs. Since tension on the Korean Peninsula remained high, the United States continued to station troops in South Korea.

In 2005, Wu Dawei, China's chief negotiator, attended the six-party talks in Beijing to discuss North Korea's nuclear-arms program. The United States was worried about the possible threat from China, that is, either through isolation, an asymmetric strategy, or by its blocking of enemy actions using multinational organizations. In a symbolic move, South Korea's delegates stayed in a different Beijing hotel than the Americans and Japanese, whereby the U.S. team understood that they no longer had South Korea, once a loyal ally, on their side. The Chinese team had painstakingly drawn up a fifth version of the draft accord, which Wu presented on September 26. The draft implied that North Korea would be rewarded by China with a civilian light-water nuclear reactor if it dismantled its nuclear weapons. For the United States, such a gift to a rogue tyrant likes the North Korean leader Kim Jong IL had always been a nonstarter. However, the U.S. team also could not claim an ally in Russia, which was going its own way both at the six-party talks and in nuclear talks with Iran. Thus, the crucial meeting ended up breaking down [40].

Beijing has also exploited its power advantage in other ways. It kept Washington from attending the inaugural East Asia Summit held in Malaysia in December, where the attending countries' officials talked about an Asian regional trading bloc.

China's growing sway at the bargaining table extends beyond Asia, and Washington finds itself in the uncomfortable position of having to work harder to impact countries than it once did. That was the case recently in Vienna, when the United States and its European allies had to lobby intensively for a resolution by the board of governors of the International Atomic Energy Agency (IAEA) to refer Iran's nuclear program to the

U.N. Security Council. China, a board member, decided to abstain, along with Russia. However, a whole new round will be played out at the meeting of the Security Council, where Beijing bears a critical veto [40].

Figure 4. Map of Vietnam (From: The History Place, http://www.historyplace.com/unitedstates/vietnam/index.html, Accessed on September 11, 2005).

D. VIETNAM WAR (1954–1975)

In July 1954, Vietnam Communist forces defeated the French armed forces, a critical battle that convinced the French that they could on longer maintain their power in Vietnam and were forced to leave. Later, France and Vietnam signed a peace agreement, the Geneva Peace Accords.

Vietnam's delegates to the Geneva conference, under the shadow of the Korean War and outside pressure from the Soviet Union and China, agreed to the temporary partition of their nation at the 17th parallel. In 1956, Ngo Dinh Diem won a controversial election that made him president of South Vietnam. He urged the United States to support his counterrevolutionary alternative, claiming that the North Vietnamese wanted to take South Vietnam by force.

In late 1957, with American aid, Ngo Dinh Diem began his counterattack. In 1961, President John F. Kennedy sent a team of American advisers to South Vietnam to report on conditions there (December 1961 White Paper) and to assess possible future American economic, technical, or military aid requirements. Kennedy chose a middle route that did not interrupt the Vietnam civil war with a U.S. use of military force. In August 1964, in response to American and South Vietnamese espionage, North Vietnam was reported to have launched a locally controlled attack on two American ships in the Gulf of Tonkin. After President Kennedy's assassination, the United States changed its policy toward Vietnam. The continuing political problems convinced the new president, Lyndon Baines Johnson, that more aggressive action was needed. After the alleged communist attacks on the two U.S. ships, in August 1964, the Tonkin Gulf resolution was passed by the U.S. Senate at the request of President Johnson, and U.S. military aid to South Vietnam increased.

Meanwhile, the Chinese Communist Party leaders were paying close attention to Vietnamese communist revolution. Mao Zedong, Zhou Enlai, and other Chinese leaders had developed close relationships with North Vietnam's leader, Ho Chi Minh. China's determination to offer material and manpower to North Vietnam was based on a combination of strategic and ideological considerations. China's leaders realized Vietnam's strategic important to the security of China's southern border. Beijing considered Vietnam, along with Korea and Taiwan, as the most possible places where the United States might build its bases and initiate military hostilities [41].

Despite massive U.S. military aid, heavy bombing, and the growing U.S. troop presence, Vietnam was unable to defeat the North Vietnam military force. In 1968, after President Johnson's decision not to seek reelection, serious negotiations to end the

Vietnam War began. But things changed when the new president, Richard M. Nixon, was in charge of the Vietnam issue. In a drastic change from previous U.S. tactics, Nixon combined U.S. troop withdrawals with intensified bombing and the invasion of communist sanctuaries in Cambodia in 1970 [11]. The fighting between South Vietnam and North Vietnam continued despite the peace agreement until North Vietnam launched another offensive in early 1975. After South Vietnam's request for help was denied by the U.S. Congress, the South Vietnamese forces soon collapsed, and in April 1975, North Vietnamese troops marched into Saigon. Vietnam was reunified in July 1976, and Saigon was renamed Ho Chi Minh City.

Beijing began to withdraw the Chinese troops from Vietnam in early 1969 but promised Hanoi that China's troops would return if the United States came back. From China's perspective, Beijing's support for Hanoi's war of communism revolution would serve to break "the ring of encirclement" by the United States and thus enhance the security of China [41].

The danger of war between the U.S. and the China was real because China was ruled by ideological dogmatists who would soon have nuclear weapons at their disposal and who, though far more ferocious in words than in actions, nonetheless were intensely hostile to the United States. In the short run, the danger of war between China and the United States was real because the "open-ended" war in Vietnam could bring the two great powers into conflict with one another, by accident or by design, at almost any time. As a result, in July 1971, President Nixon made a formal visit to China to seek a more normal relationship with China and thereby avoid China's direct involvement in Vietnam.

In its own involvement in Vietnam, the United States obviously failed to understand the tactical nature of Vietnamese fighting. The North Vietnam used guerrilla war, or People's War, as its asymmetric military strategy, so the United States' superior military strength was not the main key to achieving victory. Guerrilla war, or People's War, is a very peculiar type of war, one that is very difficult for Western countries to figure out. In this kind of war, modern weapons may not determine which side will win or lose. The crowd's will and the people's determination are the key factors in achieving victory. Such a new idea, like the general thinking of the communist countries, was

opposite to the thinking of the noncommunist countries, which believed that only military strength could decide who won or lost. But guerrilla war is not enough, it cannot defeat traditional forces, it can only cause a military deadlock. A deadlock, however, will result eventually in a political solution. When a conflict is solved politically, the traditional forces always suffer a greater loss. Because of the loss of human life and property that guerrilla forces need to stand are within the range that can be stood. But the traditional forces must be able to afford economic expenses that are extremely high.

As time passed, the United States found it difficult to explain to its people why it still could not resolve the Vietnam issue after the loss of so many American and Vietnamese lives. U.S. is not suited to making long-term war, especially fought for another country. As long as the U.S. military stayed “one day more,” it would bear more injuries and deaths. Moreover, as the war was between two sides of the same country, the North Vietnamese could excite nationalism as a means to defeat an outside force, the United States.

The Vietnam War provided an excellent example for China. The United State’s military strength could neither win nor lose on the battlefield. Thus, China began to focus on the possibilities of fighting the United States, if necessary, with advanced information technologies and long-range precision weapons. China’s current doctrine emphasizes “People’s War under modern condition” and “local wars under high-tech condition.” This emphasis has surprised many Western followers of Chinese policy, who believed those ideas had lost relevance in the information age. In fact, in China’s view, their significance has increased [36].

Today, China uses electrons such as computers and network systems to practice its new asymmetric military strategy, and it firmly believes that its asymmetric strategies are superior and thus can compensate for its technological deficiencies over the United States. As a result, electronic, computer-software and -hardware, and communications-and-information engineering experts will possibly become the genuine heroes of the new People’s War, much like guerrilla warriors in the past.

In addition to economic factors, this explains why China is willing to reduce its army. China can keep up with other countries, such as the United States, by employing a

large number of information engineers and citizens with computers instead of soldiers. China clearly has the people to conduct a “take-home battle”: a battle conducted with computers at home would allow millions of citizens to hack into U.S. Department of Defense (DoD) computer and network systems when needed [39].

Figure 5. Map of the Taiwan Strait and Taiwan (From: Infoplease: http://www.infoplease.com/atlas/country/taiwan.html, Accessed on April 10, 2006).

E. TAIWAN STRAIT CRISIS

On August 1958, China suddenly launched a large-scale artillery attack on Jinmen (Quemoy) which lasted for forty-four days due to the distance between Quemoy and mainland China was less than 5 km. Jinmen is both an island and a group of islands and twelve islets off southeast China in the Taiwan Strait. The islands are heavily fortified and have been administered, along with Matsu, by Taiwan since the Chinese Revolution of 1949. [From: www.thefreedictionary.com/Quemoy, Accessed February 10, 2006.] The United States assisted Taiwan, but only with limited logistic support: U.S. military ships escorted Taiwan supply ships within the three-mile neutral limits off Jinmen. Because China had military-supply problems, it announced an “even-day" ceasefire,” and soon after, a permanent ceasefire. The attack launched by the PRC was temporarily over, but

this military action proved that China was eager to reunite Taiwan with the mainland by military force.

Due to the tension between China and Taiwan, when John F. Kennedy became President (1961–1963), he was afraid of involving the United States in a war in the Taiwan Strait [2]. On June 27, 1962, Kennedy issued a statement that the U.S. assistance to Taiwan would be restricted to defense. The United State would not support any attempt by Taiwan to attack China.

In July 1971, then-President Richard M. Nixon made a formal visit to China. Many countries explained this action as an indication that the United States wanted to cut off its relations with Taiwan. Consequently, the U.N. voted for China to take Taiwan's place at the United Nations, and, in l971, Taiwan vacated its position. In December 1978, then-President Jimmy Carter formally announced that the United States would establish formal diplomatic relations with China on January 1. Thus, on that date, the United States simultaneous ended its formal diplomatic relations with Taiwan and began to withdraw U.S. military troops stationed there [2].

Nearly forty-six years after Chiang Kai-shek established his government on Taiwan, China still regards the island as part of the mainland and is concerned about the island's potential for claiming its independence. As the Taiwanese become more powerful, the likelihood increases that Taiwan will grow less interested in reunification and more interested in international recognition. Today, while twenty-eight countries recognize Taiwan, there has been a subtle shift toward more support for China. China believes the Taiwan authorities have given up on the one-China principle and now put forth a two- China theory, to be achieved in stages. The United States has denied the PRC's right to use force against Taiwan for the purpose of unification. Nonetheless, China will use any way it can to stop Taiwan from gaining its independence from China's mainland sovereignty. China wants to ensure that Taiwan remains part of the motherland and not one of the "lost territories."

For more than a decade, Taiwan's military modernization effort has focused on acquiring modern weapons systems and associated equipment to deter China's aggression. The Republic of China government has spent billions of dollars on domestic

programs like the Indigenous Defense Fighter (IDF) and the Tien Kung air defense system, as well as on foreign purchases like the U.S.-made F-16 fighter plane and the French-built Lafayette-class frigate. Many of these newer systems are in the process of being assimilated into the active inventory[2].

In 2004, when Taiwan held its first democratic presidential election, China fired ballistic missiles over the island, a hundred miles from its coast. The United States responded with its biggest show of force in Asia since the Vietnam War, sending two aircraft carriers and fourteen other warships to secure Taiwan [42].

The current Bush administration is considered as more supportive of Taiwan than any previous U.S. administration since 1979 (Jimmy Carter). First, the Bush administration responded to Taiwan's annual request to purchase U.S. weapons, approving a more robust arms-sales package to Taiwan, including Kidd-class destroyers, diesel submarines, and P-3C Orion aircraft. Second, it enhanced U.S./Taiwan military-to-military contacts, including meetings between higher-level officers and cooperation on command, control, computer, communications, information, and training assistance. Third, it approved transit visas for top Taiwan officials, such as the Taiwanese president and vice president, to come to the United States [2].

China, however, interprets the U.S. and European sales of advanced combat equipment to Taiwan as hostile and destabilizing acts that will destabilize the balancing power between China and Taiwan. High-level transfers of sophisticated weapons also raise the level of tension and instability between Taiwan and China. As a result, the U.S. arms sales to Taiwan complicate U.S.–China relations.

F. SUMMARY

As China's military and economy gradually began developing into Asia's giant, the United States began to exert its considerable impact on Israel to stop its arms sales to China. In 2000, the United State intervened in Israel's planned sale of the PHALLON Airborne Warning and Control System to China. The Bush administration views China as a strategic competitor rather than a strategic partner, which is different from the United States' previous defense policy.

In the past, China planned to achieve its political objective of unifying Taiwan through deception, surprise, and decisiveness, strategies that would have caused instability in the Taiwan Strait region. However, on April 10, 1979, Taiwan and the United States signed the Taiwan Relation Act (TRA), which assured a U.S. commitment to a peaceful resolution to the Taiwan question. The Act also gave the United States the power to use military force to aid Taiwan and deter possible Chinese aggression.

Consequently, China's military strategists continue to raise the issue of possible U.S. intervention, because the United States does not support China's taking Taiwan by force. Following the old Chinese military strategist Sun Tzu's concept of "overcoming the superior with the inferior," China gradually developed asymmetric warfare as its military policy for confronting the United States.

In recent years, there has been an increasing recognition of the importance of advanced information technology (IT) in modern warfare, especially since the United States' use of it in the invasion and war in Iraq. China regards information warfare as a key strategic weapon because the potential asymmetric applications of IT can be adapted to resist a technologically superior adversary such as the United States. Web sites in China are heavily used as a means to target U.S. Department of Defense computer network systems and other U.S. agencies' operational systems (OS) and information systems (IS). Chinese hackers have successfully penetrated hundreds of unclassified networks and secret military networks. Among its concerns about China's military spending, its computer network attacks, and the ongoing modernization of its armed forces, the United States has gradually become most seriously concerned about China's increasingly well developed asymmetric-warfare capability [38].

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE PLA'S TRADITIONAL MILITARY CAPABILITY

A. THE PLA ARMY

1. Background Information

In recent decades, the PLA has implemented a number of military reforms. The purpose of these reforms has been to maintain China's national integrity, security, and sovereignty. Beginning in 1998, the former "field" armies were reclassified as "group" armies, with engineers, aviation, integral artillery, and other support groups. The main impetus for these changes is the CCP's realization that the PLA is not agile enough to cope with a fast-moving modern opponent, even within China's own territory. To address these drawbacks, the army is developing new operational doctrines and conducting an overall modernization program [15].

The United States' experience during its two Persian Gulf wars has had a definite impact on the Chinese PLA's modernization program. In the 2003 invasion of Iraq, both sides had a roughly equal number of troops: there were approximately 540,000 coalition troops to approximately 545,000 Iraqi troops. However the coalition's initial fast-moving and massive armored attack into Iraq, just to the west of Kuwait, took the Iraqis completely by surprise. Once the U.S. and allies troops had penetrated deep into Iraqi territory, they turned eastward, launching a massive flank attack against the Iraqi Republican Guard. Because this ground campaign, though relatively brief, was so agile, the coalition forces, mainly U.S. and British troops, were quickly successful with minimal losses. The Persian Gulf military action prompted the PLA to completely reorganize—not only its military structure, but also its doctrines, equipment, logistic, personnel training, military exercises, and other related policies.

The Chinese modernization program included an extreme doctrinal change stressing "high-tech local war," " joint warfare," and "mechanization." Its overall goal is to produce a ground force that is more mobile, has greater high-tech firepower, and is better able to operate jointly with other services. Emphasis is being put on upgrading the PLA's C4ISR (command, control, communication, and computer intelligence,

surveillance, and reconnaissance) capabilities, as well as the capabilities of the Special Forces, militia forces, army aviation units, and rapid reaction units.

In recent years, the PLA has also focused on building local reserve and militia capabilities to support future war efforts. The approximately 1.5-million militia force, a very crucial backup force for the PLA, is composed of ordinary civilians who retain their regular jobs and work. The primary militia comprises a rapid reaction detachment, infantry detachments, specialized technical detachments, and detachments with other specialties.

In September 2003, the PLA announced an overall personnel reduction of 200,000, which is expected to be completed by 2005. This followed a 1997 reduction of 500,000. Both were designed to facilitate the PLA military modern program. In terms of organization, this latest reduction will see the elimination of some of the group armies in the military region and a reduction of the total number of military officers in the PLA. With the rapid absorption of new communication and information technology, the PLA intends to build a fatter chain of command to reflect the future command-and-control C2 system in military operations.

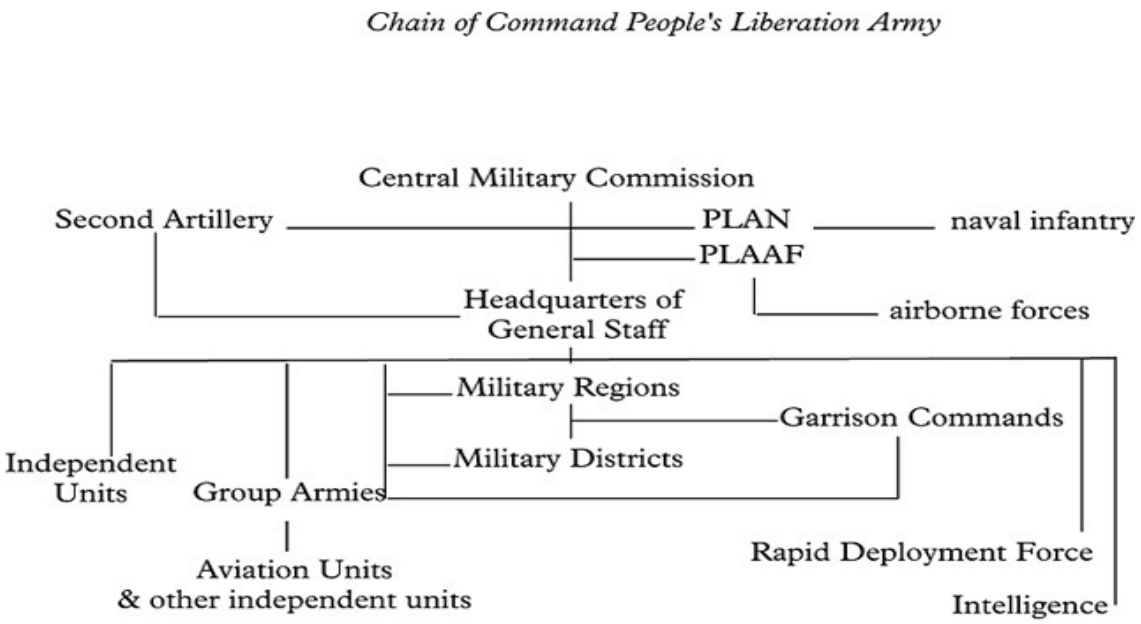

Figure 6. People's Liberation Army Chain of Command. (After: Jane's Document View 2005).

2. Special Forces

After the Unites States conducted a successful coordination between Special Forces and traditional forces to attain an overwhelming victory during the Persian Gulf War, the PLA had a better understanding of the significance of a relatively small but well-trained fighting unit with high-tech weapons employing a futuristic warfare style. Therefore, the PLA became dedicated to developing its own special force with a considerable annual defense budget and the necessary related personnel.

The PLA, traditionally, has had a small section of highly cohesive, patriotic, and physically fit troops, who are well trained in basic skills. These military forces, which receive specialized training in helicopter-landing and sea-deployment exercises, are able to operate a wide range of Chinese-made and foreign weapons. They are equipped with the most advanced sophisticated equipment to conduct a wide range of missions: guerrilla warfare, intelligence collection, reconnaissance, raids, penetration, target-facility destruction, and the capture of valuable enemy commanders.

In addition, as part of its modernization, the PLA special forces put a huge effort into Electronic Warfare (EW), as it can act as a combat multiplier. The PRC asserts that this is for the protection of China's interests; it also employ EW assets to support all echelons through the use of electronic countermeasures (ECM) consisting of active and passive jamming devices for communications targets; and electronic support measures (ESM) consisting of intercept and direction-finding systems. The PLA special forces have the capability to incorporate electronic warfare to disrupt an enemy's use of the electromagnetic spectrum during a timeframe critical to the enemy, and thus to render the enemy ineffective in achieving his objectives.

The first PLA Special Forces unit was built in the early 1990s in the Guanzhou military region, a strategic military location very close to Taiwan. In the late 1990s, a regiment-level PLA special force unit with three light tanks was established in each military region and played a role similar to rapid reaction units under the regional headquarters' direct command. Each Special Forces unit was equipped with the most modern high-tech weapons system, night-vision goggles (NVG), remote-piloted vehicles (RPV), global positioning systems (GPS), and satellite communication phones.

The 2000 annual U.S. Department of Defense (DoD) report to Congress assessing the PLA's military forces indicates that the Chinese special forces would be used primarily in the early stages of a conflict to attack key personnel and targeted infrastructures and to secure air and naval facilities to allow for a follow-on force [2].

The PLA Special Forces are responsible for carrying out several crucial tasks. First, they may do a long-distance reconnaissance to collect timely and important information from the enemy and record the battlefield-damage situation, so as to support the commander to make crucial decisions. Second, Special Forces could successfully conduct a penetration action beyond the enemy's defense line with helicopter- or special-vehicle transportation, to better understand the enemy's logistic transportation lines and military force deployment. Destroying those targets prior to launching an overall attack is crucial to an army's ultimate success. Third, Special Forces are able to launch surprise attacks or raids on civilian and military airports, wharfs, military bases, and radar alarm systems, to delay and deny the enemy's response to the current battlefield situation. Fourth, the high-tech trained Special Forces are responsible for prosecuting a computer network attack, such as a virus or backdoor program, on an enemy to destroy its C4ISR assets and cripple its C4ISR capability.

3. Militia Forces

China extends its national defense education primarily to civil servants, young students, militia members, and reservists. It is absorbed into the curriculum of both the ordinary schools and the Communist Party schools. More than 2,500 Party schools throughout China offer courses pertaining to national defense.

China's national defense education is conducted as special lectures that are different from the basic science courses. A Military Day has been adopted on all campuses as well as short-term training programs. As a result, government functionaries' awareness in performing their national defense duties is continuously enhanced. National defense education has been incorporated at different levels into the courses at all kinds of schools to provide even young students with national defense knowledge and thereby inspire patriotism.

National defense education for the militia and reserve forces is conducted in connection with political education and intensified military training. There has also been a notably greater investment in the People's Liberation Army's reserve and militia forces, estimated to number about 1.5 million [37].

Serving as backup for traditional armor, artillery, and infantry units, the militia forces are also being used to fulfill special high-tech requirements, like information-warfare and computer-network-attack units. These are drawn from the civilian computer-technician sector. Reserve and militia units are now also increasingly assigned to radar alarm, air defense, and logistic support missions.

4. Army Aviation

In the mid-1980s, the Central Military Commission (CMC) made a key decision, to develop an air mobile capability in the ground forces, and in 1986, it formed the Army Aviation Bureau. The first operational regiments were activated in 1988, with about fifty helicopters transferred initially from the PLA Air Force. Later, more helicopters were deployed into the army aviation unit. To date, ten army aviation units, including a training unit, operate a combination of Chinese-built helicopters and others purchased from the Russia, European countries, and the United States. The estimated numbers of helicopters in the army aviation units varies from 200 to 300, a very small amount compared to the size of the entire PLA Air Force.

In 2004, the Army Aviation Bureau was continuously built up within the 12 Regiment (Currently, the PLA has 10 to 12 Army Aviation Regiments). Over two hundred Russian Mi-17s will be added to the army's aviation force by 2005. A scout/attack helicopter will be put in service by the Z-11 and WZ-11. The armed Z-11 , carried low-light/auto-tracking targeting sensors, began flying in late December 2004.

5. Rapid Reaction Unit

In 1985, China implemented a fundamental transformation of its military strategy, based on its assessment that the improving relationship between the United States and the Russia had greatly reduced the probability of another world war.

In June 1985, Deng Xiaoping, chairman of the Central Military Commission, stated: "there will not be large-scale warfare in the foreseeable future." And he

subsequently converted the strategic doctrine of the PLA from a "People's War under Modern Conditions" to" limited war under high-tech war conditions" [2]. In contrast to the previous concept of a People's War that "traded space for time," this new doctrine focused on the possibility of either a major conflict or a limited war along China's borders. As a result, officials of the PLA's management set goals for the enhancement of two main military capabilities:

1. The capability of advanced strategic-weapons systems to exert an effective deterrence, such as unclear weapons and long-distance cruise missiles.
2. The army's capability to develop highly competitive, high-tech oriented Rapid Reaction Units (RRU), with the most advanced equipment and more training opportunities than regular units, to deal with small-scale, highly intensive regional combats in the future.

The PLA evaluated the situation efficiently and effectively and in keeping with the new strategic doctrine. It initiated crucial organizational-structure reform to effect the establishment of Rapid Reaction Units in the mid-1980s. The PLA specified four group armies — the 38th, 39th, 54th, and 23rd — as RRUs, to be provisioned with mobile vehicles, electronic warfare equipment, and modern logistic support.

The RRUs have two main roles. The RRUs could be sent to an area where a conflict initially occurs. For instance, the RRUs could serve as defense units in cases of internal disorder, such as in Tibet, Xingjian, and the Taiwan Strait. The RRUs' other role is to improve China's responses to external environment issues, such as, for example, in the South China Sea or Taiwan or on the Korean peninsula.

B. THE PLA NAVY

1. Background Information

In 1949, Mao, as chairman of China's Central Military Commission (CMC), asserted that "to oppose imperialist aggression, we must build a powerful navy" [20]. And, in March 1950, a Chinese Navy Academy was set up at Dalian. Most of its instructors came from the Soviet Union. In September 1950, regional naval forces were formally established under the command of the General Staff Department. The PLA navy's ships and boats were mostly acquired from the old KMT government's naval forces. Two years later, a naval air force joined the naval active service. In 1954, approximately 2,500 Soviet Union naval advisers and military officers were sent to China

along with modern and sophisticated warships. Due to the Soviet Union's strong military assistance, between 1954 and 1955, the PLA navy was reorganized into a North Sea fleet, an East Sea fleet, and a South Sea fleet.

In the 1950s, when it was first established, the PLA navy received and imported military equipment and shipbuilding technology primarily from the Soviet Union, until it gradually developed the ability to make some specific components of naval equipment itself. In respect to shipbuilding technology, at first, the Soviet Union assisted China in building vessels; later, China copied the Soviet Union designs to manufacture vessels; and, finally, China produced vessels of its own design.

The Navy grew dramatically in the 1970s when approximately 20% of the defense budget was allocated to maritime warfare. China's fleet of traditional submarines was increased from thirty-five to a hundred, its missile-carrying ships increased from twenty to two hundred, and larger surface ships, including support ships for oceangoing operations, were also produced. The navy also began to use newer military technology to develop its nuclear-powered attack submarines and ballistic submarines.

In the 1980s, the navy continued to develop into a regional naval power with some green-water capabilities. The navy's modernization efforts encompassed higher educational and technical standards for personnel and a reformulation of the traditional coast defense doctrine and force structure, in favor of more blue-water operations and training in naval combined-arms operations involving submarines, the surface fleet, naval aviation, and the coast defense force.

Naval operations may be framed in terms of maritime geography, usually under four categories. These categories designate operations ranging from inland waters to global deployments by large, relatively self-sufficient fleets.	
Type	**Definition**
riverine	From inland water to the coast
brown water	Reaching from the coast to about 200 nautical miles seaward
green water	Refers to ocean areas, from the seaward end of brown water to a point marked by the Caroline Islands and other islands, about 1,800 nautical miles from the coast
blue water	Refers to the remaining global ocean areas

Table 3. Four Categories of Maritime Geography (From: http://www.globalsecurity.org/military/library/report/2003/pla-china_transition_11_ch07.htm, **A**ccessed on September 30, 2005).

In 1982, the PLA navy conducted a successful test of an underwater-launched ballistic missile; in 1984, it extended its naval operations in the South China Sea; and, in 1985, it visited three South Asian nations. From 1986 on, the navy also had some success in developing a variety of ship-to-ship, ship-to-shore, shore-to-ship, and air-to-ship missiles, as well as its capabilities for antisubmarine warfare, electronic warfare, and naval aviation. At present, the PLA navy consists of the naval headquarters in Beijing and three fleet commands: the North Sea fleet, based at Shandong; the East Sea fleet, based at Shanghai; and the South Sea Fleet, based at Zhanjiang.

Over the last decade, the navy has modernized its forces by eliminating large numbers of older ships and replacing them with fewer, more modern units. The number of submarines has declined by about one-half. The size of the major surface combatant fleet has been relatively stable, with older ships slowly being replaced by newer China-built destroyers and frigates. Nearly all of the navy's inventories of U.S.-built, World War II–vintage landing ships have been replaced by similar numbers of domestically produced vessels.

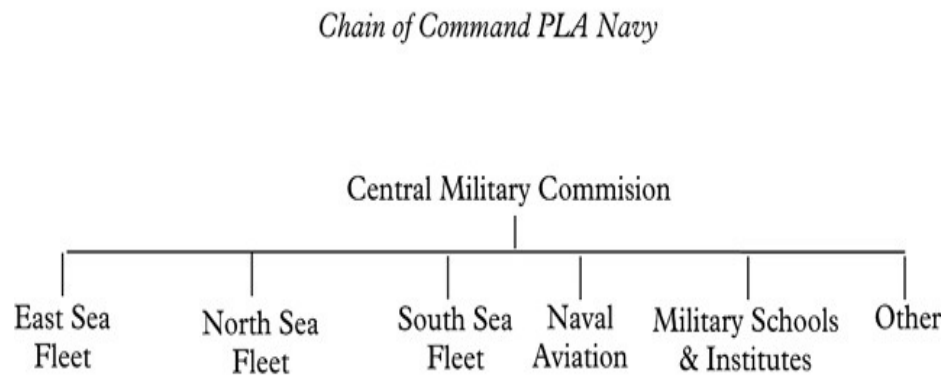

Figure 7. People's Liberation Navy Chain of Command. (After: Jane's Document View, 2005).

2. Active Offshore Defense

Traditionally, the PLA navy was considered as a ground-force assistant. Therefore, the navy's doctrines put an emphasis on coastal defense. General Liu Huaqing, head of the PLA Navy head from 1982 to 1987 and Central Military Commission vice chairman from 1988 to 1997, called for expanding the navy's operations from coastal defense to active offshore defense.

Two factors were active in the PLA's strategic move to focus on the issue of an active offshore defense. One factor was China's economical interests in the South China Sea, which encompasses a portion of the Pacific Ocean stretching roughly from Singapore and the Strait of Malacca in the southwest to the Taiwan Strait in the northeast. This area includes more than two hundred small islands, rocks, and reefs, with the majority located in the Paracel and Spratly Islands chains. The islands are important for both strategic and political reasons, because ownership claims to them are used to bolster claims also to the surrounding sea and its resources. This is significant because the South Sea is rich in natural resources, such as oil and natural gas that continue to garner attention throughout the Asian–Pacific region.

Asia's economic growth rates are among the highest in the world, and the economic growth is accompanied by an increasing demand for energy. China alone accounts for more than one-third of the world's oil consumption [20]. Much of the additional demand will need to be imported from the Middle East and Africa. Excluding cargoes bound for South Asia, most of that volume will pass through the strategic Strait of Malacca into the South China Sea.

Countries in the Asia–Pacific region depend on seaborne trade to fuel their economic growth. And every year, more and more merchant ships sail through the South China Sea. The economic potential and political importance of the sea has resulted in chaos in the surrounding nations, which claim this sea and its resource for themselves.

Another factor is what China perceives as an increasing threat from its maritime neighbors. Three such potential threats are 1) from South Korea, which crosses the Bo Hai (Po Hai, or Gulf of Chih-li, an arm of the Yellow Sea, northeast China); 2) from Japan, which is very close to China; and 3) from Taiwan, which is within 100 nautical miles.

The meaning of "offshore" is not always obvious. It can be defined as a range from the coast to coastal operations within 100 nautical miles of the shoreline, or as the 700 nautical miles required to patrol the South China Sea's Spratly Islands chain. The range of "offshore" for the PLA navy is linked to its own weapons system. The Chinese military's longest-range, shore-based system includes two main surface-to-surface

missiles: the HY-2 with a 52-nautical-mile range and the HY-4 with an 84-nautical-mile range. In addition, the navy's B-6 bomber has a combat radius of 1,700 nautical miles.

3. PLA Amphibious Units

The PLA navy's amphibious fleets have only enough capacity to transport about one infantry division. The navy also has many small-size landing craft, troop transports, and barges, all of which could be combined with civilian trawlers, merchant ships, and fishing boats to practice tactic operations.

As a rule, in the navy's experience, in an assault, the attacker needs five times more troops than the attacked. So, since 1994, the PLA navy has conducted several joint military exercises with other services in amphibious maneuvers around its coastal islands. The exercises' main purpose is to increase the amphibious units' skill in conducting amphibious maneuvers, so as to enhance China's chance of taking Taiwan by force and preventing U.S. intervention in the Taiwan Strait.

Currently, the PLA navy has a military force for amphibious maneuvers that consists of two brigades, with approximately 10,000 troops belonging to the South Sea fleet, one of the PLA's excellent rapid-reaction units equipped with a Type 63 amphibious tank, Type 7711/7712 amphibious armored personnel carriers, Type 54 artillery, and anti-tank missiles. The most important drawback to this amphibious unit is its lack of long-range lift, logistic support and superior air support, which hinders the navy's ability to project its amphibious force. However, as the navy modernizes and moves to a blue-water naval force, it will not only be a serious threat to Taiwan but also a strong challenge to the United States in the Asian–Pacific region.

4. The PLA's Naval Capability

In a contest with a strong opponent, especially the United States, the PLA navy will rely on its speed, mobility, and flexibility. Its main goal will be to deploy enough naval strength to challenge U.S. navy in a limited regional scenario.

Since 1970, the Chinese navy has become possibly the third-largest navy in the world. It has enormously increased it number of active-duty members and ships and upgraded its academic training projects. This maritime awakening is the effect of major

changing economic objectives, military-strategic considerations, and increased government support.

The PLA navy's weaknesses are outdated weaponry, outmoded electronic systems, conventional propulsion, naval aviation, mine warfare, and situational awareness, that is, knowing the location of one's own forces and those of the opponents. Situational awareness and electronic systems are especially critical for achieving effective reconnaissance, surveillance, and intelligence collection. The PLA navy has not been able to achieve this strength.

Currently, it has more than fifty active, medium-sized or large, surface warships, but only a few have modern capabilities. The navy's most capable ships are one Sovremenny-class, one Luhai-class, and two Luhu-class guided-missile destroyers and seven Jiangwei-class frigates, which have a potent anti-surface-missile capability and cruise-missile batteries. Their antisubmarine systems are limited. Furthermore, the PLA's ships could be viewed as relatively expendable in a Taiwan scenario, since the nearby mainland provides ample air and missile power.

Type	Class	Displacement	1985	2000	2010
Destroyers			**15**	**21**	**27-29**
Type 956	Sovremenny	8,480	-	1	4
Type 054	Luhai	6,600	-	1	5
Type 052	Luhu	5,700	-	2	2
Type 051	Luda	3,960	11	17	~ 11
Type 07	Anshan	2,040	4	-	-
Frigates			**31**	**36**	**34-43**
Type 054	Maanshan		-	-	8
Type 059	Jiangwei III	3,000	-	-	3
Type 057	Jiangwei II	2,250	-	2	6-8
Type 055	Jiangwei	2,250	-	5	4
Type 053	Jianghu	1,925	20	28	~ 25
Type 053K	Jiangdong	1,925	2	1	-
Type 065	Jiangnan	1,400	5	-	-
Type 01	Chengdu	1,510	4	-	-
Guided Missile Boats			**100**	**83**	**55**
Type 520T	Houjian	520	-	4	4
Type 343M	Houxin	478	-	14	~36
Type 021	Huangfeng	205	100	65	~25

Type	Class	Displacement	1985	2000	2010
Submarines			**117**	**66**	**62**
Type 094	NEWCON SSBN	8,000	-	-	8
Type 092	Xia SSBN	6,500	1	1	-
Type 093	NEWCON SSN	6,500	-	-	4
Type 091	Han SSN	5,500	3	5	5
	Kilo	2,325	-	2	4
Type 039	Song	2,250	-	2	5
Type 035	Ming	2,100	2	16	20
Type 033	Romeo	1,710	90	38	15
Type 03	Whiskey	1,350	20	-	-
Type 031	Golf SSB	2,700	1	1	-
	Wuhan	2,100	-	1	1
Amphibious Warfare			**4**	**15**	**29**
Type 074	Yuting	4,800	-	6	20
Type 072	Yukan	4,170	3	7	7
	Yudeng	1,850	-	1	1
Type 073	Yudao	1,460	1	1	1

Table 4. PLA Navy Capability (From: http://fas.org/man/dod-101/sys/ship/row/plan/index.html, Accessed September 30, 2005).

C. THE PLA AIR FORCE

1. Background Information

As China is the most powerful country in Asia and an emerging super power, its neighbors pay serious attention to its military procurement plans. Despite conflicts in the region, the China's military reform is gradually casting a shadow over those neighbors' own plans for military procurements.

According to information from the U.S. Office of Naval Intelligence (ONI), two new fighter planes are being developed and manufactured for the People's Liberation Army's air force (PLAAF) [17]. One is the J-12, which is similar to the U.S. F-15 long-range, multi-role fighter. The other is the J-10, which is comparable to the U.S. F-16. At the same time, China is forging ahead with its integration of Russian Su-27 fighters into the PLA air force. The first batch, procured from Russian in 1992, provided the air force with its first-ever long-range defensive and offensive counter-air strength. A second batch of twenty-four fighters followed in mid-1996.

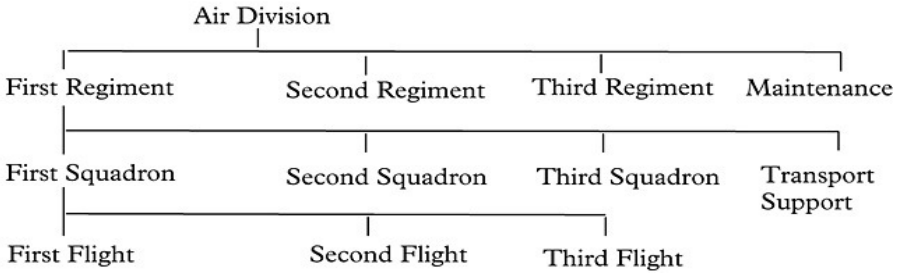

Figure 8. People's Liberation Air Force Chain of Command. (After: Jane's Document View 2005).

2. Attack Aircraft

The most important attack aircraft in China's air force are its Su-30MKKs, which are deployed in two operational regiments, located in the Guangzhou and Nanjing military regions. From those locations, their range extends to Taiwan and is also a threat to U.S. military bases in Japan. All of the Su-30MKKs carry aerial-refuel probes, a functionality that further increases their strike and raid range.

The Su-30MKK was also China's first all-weather attack aircraft with a self-guided air-to-air missile. According to the air force's plans, all the Su-30MKKs will eventually be upgraded to the MKK2. That will enable the PLA to use them in naval attack missions and in joint operations, the warfare style of the future.

In the future, the air force will use the J-10 multi-role fighter and later models of the J-8 II to conduct all-weather precision attack missions. The PLA will also purchase the updated JH-7A attack aircraft. Though it is lighter and less capable than the Su-30MKK, it features fly-by-wire controls, an advanced multi-function display cockpit, an external sensor and designator pod, and will be armed with laser-guided bombs, a range of free-fall weapons, and wing-tip mounted air-to-air missile. Some JH-7As will also be armed with air-launched missiles. According to a PLA air force report, a unit of JG-7As was delivered in the Nanjing military region in early 2005. In addition, the upgraded Q-5 attack aircraft with new engines, avionics, and sensors are able to deliver laser-guided bombs, and thus fulfills the PLA's close-support mission requirement.

A possible new attacker for China's air force is the LFC-16 single-engine canard fighter. The LFC-16 uses a canard/delta and novel "side-stake" surfaces to obviate the need for expensive fly-by-wire controls.

Once special-missions aircraft, such as AWACS (Airborne Warning and Control System), tanker, and UAV aircraft, are fully integrated with the advanced fighters, the PLA air force will gradually become an effective and efficient fighting force.

3. The Airborne Forces

From the PLA Airborne Corps's prospective, the agility, flexibility, and mobility of the Airborne Corps enables it to conduct the first wave of attack in a Taiwan Strait scenario. However, the terrain of Taiwan is long and narrow and Central Mountains divides Taiwan into a west and east region. If the 15th Airborne Corps—a highly trained unit equipped with more advanced weapons than the entire Chinese army—could conduct a surprise attack and successfully penetrate Taiwan's air defense system, it could then capture crucial targets, including military/civilian airports, highways, bridges, and railroads. The Taiwan army would probably be divided in several areas, which would reduce Taiwan's counterattack capability.

Based on these considerations, the PLA leadership is considering increasing its airborne forces into a strategic strike force capable of delivering a decisive blow like the capture of a major Taiwan city such as the capital, Taipei. Thus the PLA has increased its investment in the airborne forces and reduced the total troop strength by 200,000. In addition, it has shifted some army units in order to organize a second airborne unit (possibly to be named the 16th Airborne Corps, or just considered an expansion of the 15th Airborne Corps).

According to the 2005 Jane's Document View, the PLA 15th Airborne Corps is now formally under air force control. If an emergency situation occurred, the control would shift from the air force to the Central Military Commission. There are three airborne divisions in the 15th Airborne Corps, for a total of approximately 35,000 troops.

Although the air force does not have enough airlift capability, the 15th Airborne could conduct a local airborne operation to destroy the Taiwan C4ISR system under the cover of missiles from the Second Artillery Corps. Currently, the airborne units are

receiving new air-droppable vehicles, a version of the Italian Iveco four-wheel-drive truck with HJ-9 ATGM [17] and a new lightweight "jeep," to enhance their overall capability.

D. THE SECOND ARTILLERY CORPS

In 1984, the Central Military Commission formally approved the conversion of the Chinese Artillery Corps into the Second Artillery Corps (SAC), a strategic missile force directly under the Commission's command. The SAC was established as an independent service that has the same position as the PLAAF, PLAN, and PLA Army. It was estimated to consist of 90,000 to 100,000 personnel, most of who were deployed in construction and engineering units. The remainder, which comprised less than half of the total strength, was dispatched as missile operators and guards. On average, the SAC has the highest concentration of university-educated military officers, engineers, and technicians in the PLA.

The SAC was organized into a headquarters, an early-warning division, a communications regiment, a security regiment, a technical-support regiment, and from six to seven independent ballistic-missile divisions with different personnel arrangements according to their missile type. The communications regiment provides communication systems to support from six to seven ballistic-missile divisions for combat operations.

The PLA has extensive computer simulator facilities for missile-launch operations and research and development facilities for supporting related missions. The main missile test location is in the Gobi Desert. On 16 October 1964, the PLA exploded its first nuclear device, and on 27 October 1966, conducted a nuclear missile trail. It exploded China's first hydrogen bomb on 13 July 1967. In general, the Second Artillery Corps' nuclear force was deployed to a large extent in Xinjiang Province, near Russia, Mongolia, Afghanistan, Pakistan, and Tibet.

According to Major General Yang, a former SAC deputy commander, the People's Liberty Army's future ballistic missile development must follow three steps: first, improve the survivability of its strategic nuclear weapons; second, improve the striking ability of its strategic nuclear weapons; and third, improve the penetration technology of its strategic nuclear weapons. After the PLA evaluated those goals, the

Second Artillery Corps' ballistic missiles were widely dispersed in order to increase the survivability of their launching bases. The missiles are often deployed in silos and man-made caves, including in inland China in mountainous terrain. Previously, all of the Corps's long-range ballistic missiles had been stored in fixed locations and thus were vulnerable to an enemy's first strike. Also, the SAC developed a solid fuel propellant to reduce the waiting time for launching the missiles. It is believed that the Second Artillery Corps also controls China's emerging long-range and strategic missile forces. They were so cleverly camouflaged that, for a long time, U.S. military reconnaissance satellites failed to detect their exact location. It is possible that the United States has yet to discover all China's missile-base deployments.

In recent years, the PLA put an emphasis on land-, air-, and sea-based strategic nuclear-missile launching platforms. The sea-based strategic nuclear missile can be launched by a strategic ballistic-missile submarine (SSBN); air-based strategic nuclear-missiles can be launched by the PLAAF bomber. The SAC is attempting to provide its short-range ballistic missiles (SRMB) with a GPS capability compatible with the Russian global-positioning satellite system (GLONAS). The SAC not only poses a potential threat to the United States, it has also become one of the most advanced nuclear forces in the world.

E. SUMMARY

Modernization of its military equipment has become the PLA's number-one priority. The government leadership in Beijing also has a strong desire to produce the new equipment indigenously, and they continue to pour more and more money into their defense industries in the hope of producing the necessary modern equipment within their own country. However a lack of resources and the slow conversion of China's defense industries have pushed them to purchase high-tech weaponry systems from foreign countries in the hope of "reverse-engineering" [6] the technology. Meanwhile, they have also purchased dual-use technologies from private international companies in hopes of converting the concepts or devices to a military application.

China's has experienced a change in its national priorities: its military modernization effort has become secondary to the development of the national economy. As a result, its indigenous defense-production capabilities have not obviously improved.

Its practice of acquiring complete systems from foreign sources has not produced a great increase in China's military capabilities because of the many technical bottlenecks that must be overcome. In addition, it is a time-consuming process, and their technicians also lack the ability to completely reverse-engineer them.

In sum, the China defense industry continues to face a number of significant obstacles to his development plans. First, the cutback of more than one million troops from the PLA has reduced the amount of material needed for the military. Second, the number of combat aircraft orders has fallen considerably. Chinese aircraft lack many necessary technologies, such as an electronic warfare capability on the modern battlefield; so the air force has been procuring Russian fighters such as Su-30MKKs. At the same time, they've decreased orders for the older generation aircraft produced by their indigenous defense industries. Third, China is not getting as many "low-tech" arms-export orders from third-world countries since the onset of the Persian Gulf War, which means a significant cut in revenue.

According to the 1996 Rand Corporation Strategic Appraisal, China will likely require a significantly long time (i.e., at least fifteen to twenty-five years) to attain a truly modern force structure and an operational capability sufficient to challenge the U.S. military presence in the region" [59]. There seems little possibility that China will achieve indigenous advanced-weapon production in the near future. Moreover, several of China's advanced weapon systems came from Russia and Israel, and many spare parts for those systems are not readily available. It takes many months to get spare-parts orders filled for those advanced aircraft and weapons. Thus, all in all, China's military modernization effort, in contrast to its economic reform, has been very slow.

From China's viewpoint, the United States seems determined to prevent China from challenging its preeminent position regionally and globally. One obvious example of this is the arms embargo that the United States and its European allies put in place against China and the prohibition of certain advanced technologies, especially dual-use technologies, being transferred from the United States itself. Perpetuating the separation of Taiwan from mainland China is also considered to be an important goal of the U.S. strategy. Taiwan's abundant information technology resources and strong economic

power along with its 20 million people, once reunited with the mainland, would be like adding wings to a tiger [37].

U.S. efforts to improve relations with countries on China's periphery will put the United States in a better position for strategic competition with China in the future. The recent strengthening of the U.S.–Japan military alliance, including new Defense Guidelines, enhanced the United States military arrangements with several Southeast Asian countries as well as with the Central Asian countries bordering China. In addition, the United States plans to deploy a theater missile defense (TMD) system in the region encircling China. Discussion of the possible inclusion of Taiwan in that "region-wide" U.S. defense missile system on China's periphery also has intensified China's suspicion that the United States views China as a likely strategic adversary in the coming years. In all, these factors are driving China to consider an alternative strategy using asymmetric warfare capabilities to challenge U.S. hegemony and to secure a dominant position both in Asia and in the world at large.

IV. PEOPLE'S LIBERATION ARMY'S MILITARY MODERNIZATION

A. THE GOAL OF MILITARY MODERNIZATION

Among the many uncertain factors of Asian regional stability and security, none is more compelling than China's military modernization. The combination of its military improvements and its economic growth demonstrates that China is attempting to secure a dominant position in Asia.

Historically, Asia has focused on stratagems, while Western nations have focused on technology. Thus, when an Asian military force faces a difficult situation, it seeks solutions in stratagems to make up for its technological deficiencies. When a Western military force faces a difficult situation, it often finds a solution through technological means [36]. It is not surprising, therefore, that China's military modernization is not focused so much on updating its technology but on updating the Chinese military's strategy to fit modern technologies.

There has been some progress in this regard in the PLA army. Most of the PLA's group armies now have designated rapid-reaction units that receive the most advanced training and the most sophisticated equipment. This gives China the ability to deploy and conduct limited amphibious maneuvers beyond China's border, for instance, in the South China Sea and the Taiwan Strait. The rapid reaction units are small, however, and are dispersed throughout the country, and their lack of lift capability limits their effectiveness for large-scale operations [6].

The PLA air force is trying to deal with the strategic airlift problem. It received twenty-six Su-27 fighters from Russia and, in 1995, began integrating a long-range-transport operation into the training cycle to support rapid reaction units with a strategic airlift advantage. Although the Su-27 fighters provided a clear qualitative gain, their lack of an aerial refueling capability reduces their overall advantage. Although China has purchased transport aircraft, the number is so small that the air force still cannot conduct significant operations very far beyond its borders.

The PLA navy is replacing or improving its old surface combatants and its submarines. It has also received a Kilo-class submarine from Russia, which allows the navy to now operate farther from the coast for a longer period of time. However, this progress does not solve the basic problems of the Chinese navy—its inability to mount sustained, coordinated operations and to protect itself while doing so.

The PLA Second Artillery Corps continues to upgrade its nuclear weapons and continues to view nuclear weapons operations as a remote possibility. Also, it has developed a solid-fuel missile with MIRV capability (multiple independently target-able re-entry vehicles), capable of reacting to nuclear strikes from hostile countries. However, due to the catastrophic effect on both countries of a nuclear exchange, in the current situation, using specialized equipment and software in an IW (information warfare) operation to disrupt, sabotage, and destroy information in the enemy's computer-network systems is a more practical and appropriate strategy.

In general, the Chinese army, air force, and navy do not permit their forces to operate far outside of China. Given those restrictions, the PLA has identified several things that China must do to improve critical capabilities and achieve the desired military modernization:

1. Develop anti-submarine warfare, ship-borne defense, sustained naval operations, and amphibious warfare capabilities.
2. Improve the ground forces' mobility, logistic support, and air defense.
3. Build a new generation of fighters for air superiority, incorporating capabilities of strategic airlift, all-weather operation, aerial refueling, and ground attacks.
4. Improve the PLA's command, control, communication, and computer intelligence, surveillance, and reconnaissance capabilities (C4ISR).
5. Reform its military education and training systems.
6. Implement a military reserve system.
7. Use its information warfare capability as an asymmetric weapon.

In spite of its selective improvements, the PLA is not yet capable of a sustained force projection at any distance from China's borders. Thus, the PLA cannot seize and hold territories in the South China Sea. If its force were to operate in the Spratly Island chain, it would be vulnerable to significant air and sea counterattacks by U.S. forces [20].

In the first Persian Gulf War, the U.S. military forces demonstrated dramatically its ability to use advanced military technology, including precision-guided bombs, stealth technology, airborne command and control systems (C2), space-based intelligence, early-warning systems and a real-time C4ISR capability. Since the end of the war, the dependence of U.S. forces on technology makes the United States susceptible to attack by a variety of asymmetric information-technology tactics. In light of those observations, the Chinese government decided the use of information and electronic warfare is a viable strategy to pursue against U.S. interests.

At present, China is developing a number of specific IW/EW applications. These include an electromagnetic-pulse missile warhead that creates an electronic shock similar to that caused by a nuclear blast and thus could be used to disrupt the delicate electronic systems of enemy weapons. There are also computer viruses that could be used against military/civilian computer networks, such as those in banking and stock-market systems, to cause social unrest and create chaos and panic in the civilian sector. A "Trojan horse" computer program, could secretly insert a malicious code into an enemy's networks to create wrong or fake information within its precision-guided bombs [34].

B. INFORMATION WARFARE (IW) AND INFORMATION OPERATIONS (IO)

1. IW/IO Strategy in China's Military Science

During the past ten years, many of China's civilian scholars and military officers have published significant work on Information Warfare and Information Operations and related topics. The Chinese IW/IO theories are in accordance with China's culture and economics and its military situation, philosophy, and terminology. China's military art also has a strong impact on these theories, which China is quickly integrating into its overall People's War concept [7].

China's information engineering specialists — those responsible for its computer software programs and hardware architecture, its network systems and Web-enabled database applications — may, like the warriors of old, be the heroes of Mao's new People's War. China could overcome the United States by employing thousands of information engineers and experts with laptops instead of soldiers with guns. China clearly has the people to conduct an "take-home battle." A battle conducted with laptops

at home would allow millions of Chinese hackers to attack U.S. Department of Defense and other U.S. agency computers and network systems when needed.

Five people have had an especially profound influence on the People's Liberation Army's IW/IO concept. For instance, Major General Dai Qingmin, director of the PLA's Communications Department of the General Staff responsible for information warfare and information operations, points out that "new technology are likely to find material expression in informationalized arms and equipment which will, together with information systems, sound, light, electronics, magnetism, heat, and so on, turn into a carrier of strategies." He defines Information Warfare and Information Operations in keeping with Chinese characteristics, which are not the same as U.S. definitions. He also breaks away from the traditional strategy's limitation, which puts an emphasis on active defense, not attack. He suggests that a preemptive attack will achieve initial information superiority and the integration of information operations with other traditional operations will give greater scope and purpose to Mao's People's War [36].

Senior Colonel Wang Baocun, who works in the Foreign Military Studies Department of the Academy of Military Science, defines Information Warfare as "A form of combat actions which attacks the information and information systems of the enemy while protecting the information and information systems of one's own side. The contents of IW are military security, military deception, physical attack, electronic warfare, psychological warfare, and Internet warfare, and its basic purpose is to seize and maintain information dominance." Wang's work is the only one issued in English; it reflects a Western view of IW in RMA. Major General Niu Li, Colonel Li Jiangzhou, and Major Xu Dehui define IW strategy as "Schemes and methods devised and used by commanders and commanding bodies to seize and maintain information supremacy on the basis of using clever methods to prevail at a relatively small cost in information warfare."

China's ancient military stratagems are, primarily, Sun Tzu's thinking. These stratagems include: "Fool the emperor to cross the sea"; "Besiege Wei to rescue Zhao"; "Kill with borrowed sword"; "Await the exhausted enemy at your ease"; "Know the

reason perfectly well." There is a strong relationship between the thirty-six stratagems and information warfare applications. Take the following several cases, for example.

Stratagem one is "Fool the emperor to cross the sea." To distract an enemy's attention from what you are really doing, use an open act, hiding your true motivation under the guise of an ordinary activity. An IW application of this stratagem would be to use common e-mail services, e-commerce, or e-business links to mask the insertion of a malicious code or backdoor program. For example, the "Love Bug" computer virus attracted U.S. citizens, believing the email came from a dear friend or family member, to open attachment files.

Stratagem two is "Besiege Wei to rescue Zhao." When the enemy is so powerful you cannot attack him directly, attack something he focuses on in order to expose his weakness. One implementation of this stratagem in IW terms might be, if you cannot use nuclear weapons against another country because of the catastrophic results for your own country, then use a computer virus to attack the servers and network systems that support its financial, military, and political systems. China, for example, could use a computer virus to attack Taiwan's computer network systems, especially in its capital, Taipei, instead of a nuclear weapons operation [2].

Stratagem three is "Kill with a borrowed sword." When you do not have the means to attack an enemy directly, attack using someone else's strength. An IW application would be sending computer viruses or malicious codes through another country, which will confuse the enemy and prevent it from discovering the identity of the true attacker. For example, China's hackers could use a foreign country's website to send computer viruses to attack local U.S. websites. This is particularly difficult if China were to "borrow" the systems of U.S. ally.

Stratagem four is "Await the exhausted enemy at your ease." Encourage the enemy to expend his energy in futile quests while you conserve your strength. When he is exhausted and confused, attack him with little effort. An IW application would be to initiate countless anonymous computer-system attacks that will keep the enemy engaged, using all his personnel and resources, in fixing the incessant problems with his computer systems [37].

Our last example, stratagem five, is “Know the reason perfectly well.” An IW application of this stratagem could be to use a legal cover to do an illegal action in order to get some hidden potential benefit. Chinese spies, under legal cover, already know, for example, that they are stealing crucial U.S. military information, but they pretend they know nothing. They take military-related data to China to uncover the weaknesses of the information system of U.S. military weapons or so they can enhance the PLA’s overall military capability.

Chin Mak, for instance, a naturalized U.S. citizen from China, who lived in Los Angeles County, was lead engineer on a research project related to U.S. Navy warship propulsion systems for an Anaheim defense contractor, Power Paragon. Chin Mak emailed secret photos and detailed reports about the research project to his computer at home. He also took computer disks from the company, and his wife helped him copy the information onto CDs and then delivered them to his brother, a broadcast and engineering director for the Phoenix North American Chinese channel. His brother took the secret documents and was schedule to fly through Hong Kong to Guangzhou, China, to attend a meeting. According to a spokesman for the U.S. attorney’s office, Chi Mak and Tai Wang Mak, along with their wives, Rebecca Laiwah Chiu and Fuk Heung Li, were charged with stealing, trying to smuggle government property, and transporting stolen products [66]. There are likely many Chinese spies living in the United States who are ready to take assignments form China under such legal cover as being a naturalized U.S. citizen.

Although the thirty-six stratagems of war were developed from the accumulated wisdom of China’s ancient history involving military, political, economic, and diplomatic conflicts, each has an individual historical background and may not be suitable to the modern world. The importance of the thirty-six stratagems is that they represent the asymmetric nature of Chinese warfare throughout history and that the PLA uses them to form its information warfare strategies. Further, the PLA integrates Sun Tzu’s thinking, the thirty-six stratagems, and Mao’s notion of a People’s War to provide the PLA a new framework for developing an IW capability with Chinese characteristics [36].

Figure 1: China's Evolving Military Doctrine

	PW	PWUMC	LW	LWUMHTC	RMA
Force structure	Single service operations; filed armies	Joint headquarters / operations; group armies	Fist units, rapid reaction units	Smaller and fewer units; more high-tech	Selective pockets of excellence?
Force size	4 million (number = strength)	unchanged	Reduced to 3 million (for better integration)	Reduced to 2.5 million	Presumably even smaller
Main objective	Homeland defense	Defend China closer to its borders and fight mobile style of war	Win local wars on China's periphery	Deter Taiwan from independence; deter US from intervention	Employ IW by bypassing all the deficiencies (electromagnetic dominance)
Main threat	USSR	USSR	Regional skirmishes	Taiwan US	US
Main limitation	Budgetary constraint	Budgetary constraint	Budgetary constraint	Doctrine-capability gap	Technology
Main catalyst	Modernization in the aftermath of the Cultural Revolution	Changing threat perception	Changing security posture	The Persian Gulf War and the end of the Cold War	Information revolution
1978-85	PD	PL			
1985-88	RD	PD	PL		
1988-92		RD	PD	PL	PPL
1992-		RD		PD	PL

Legend:

PW:	People's War
PWUMC:	People's War under Modern Conditions
LW:	Local War
LWUMHTC:	Local War under Modern High-Technology Conditions
RMA:	Revolution in Military Affairs
PD:	Primary doctrine
PL:	Preliminary doctrine
PPL:	Pre-preliminary doctrine
RD:	Residual doctrine

Source: Compiled from Dennis J. Blasko, "PLA Force Structure: A 20-Year Retrospective," in James C. Mulvenon and Andrew N.D. Yang, eds., *Seeking Truth from Facts: A Retrospective on Chinese Military Studies in the Post-Mao Era* (Santa Monica, CA: RAND, 2001), 51-86; and Paul H.B. Godwin, "Compensating for Deficiencies: Doctrinal Evolution in the Chinese People's Liberation Army: 1978-1999," in Mulvenon and Yang, *Seeking Truth from Facts*, 87-118.

Table 5. China's Evolving Military Doctrine (From: Vincent Wei-Cheng Wang and Gwendolyn Stamper, 2002 "Asymmetric War? Implications for China's Information Warfare").

2. Vulnerability in the United States

As Art Money, assistant secretary of defense for command, control, and intelligence, has pointed out, “The rest of the world realizes that you do not take the U.S. on in a military frontal sense, but you can probably bring it down or cause severe damage in a more oblique way. And that’s where the vulnerability in the U.S. resides” [53].

The growth of U.S. information technology companies — IBM, HP, Compaq, Cisco, Microsoft, and so on —means, in effect, the development of thousands of software applications, hardware, wireless communication devices, and advanced network equipment. It helps directly to spread Internet use among the entire U.S. populace: many individual users now have several PCs at home as well as at their workplace. At the same time, the vulnerabilities of new software versions also continue to grow. Over time, the level of sophistication required to hack into an information or operational system has decreased dramatically, both the quantity and availability of hacking tools has increased substantially; and the quality has improved greatly. Overall, these factors have created an environment in which even teenagers can successfully infiltrate defense department and other U.S. government systems [35].

Thus, IT is a double-edged sword. It not only makes life easier but also results in huge economic losses for the United States from the damage caused by hacker-inspired events. Combating the Love Bug virus worldwide in 2000, for example, cost an estimated $15 billion cost [49]. And the weapons of net-war are available for download on the Internet. Unlike the weapons of traditional warfare, the tools of this trade require no long-term acquisition, training, or fielding to mount an attack. As the typical PC has become more powerful and easier to use, China can employ those limited resources as weapons to attack anywhere in the United States without notice.

Information technology is ubiquitous, but most Americans do not realize how much information technology supports their daily activities. This hidden, though extensive, dependence makes the United States very vulnerable to information warfare. Cyberspace is a virtual environment, but one that is closely related to the real-world environment of Web-enabled database searches, online shopping, e-business, and daily credit-card use, which are very common in the United States. Cyberspace is borderless

and adds a completely new dimension to military operations. China can launch numerous asymmetric and clandestine attacks at one time — attacks that have an unlimited range and are fast, easy, and cheap.

For years, the United States has experienced unauthorized intrusion and Web hacking by teenagers, industrial espionage experts, hacker groups, and foreign professional hackers such as the Chinese. These people use many tactics, techniques, and procedures, including polymorphic viruses or polymorphic codes (after changing the encryption routine, the sequence of instructions, or other aspects of the behavior of the virus to avoid detection by antivirus scanners), worms, software vulnerability exploits (code that computer security researchers write down to exploit security flaws in software such as Microsoft Windows operating systems), backdoor, Trojan horse, denial-of-service attacks (attacks on a computer or network that cause a loss of network connectivity and services by consuming the bandwidth of victim network or overloading the computational resources of the victim system), and brutal attacks [34].

It is easy to imagine a scenario in which the U.S. global media is buzzing with reports of U.S. military systems under relentless computer-virus assault from PCs in China, which could include military logistics, transportation, and administration systems essential to deploying troops to the United States, the Korean peninsula, Japan, and other U.S. military bases. Many large U.S. commercial Web sites are flooded with connection requests, paralyzing the entire commercial activities in order to cause panic among the U.S. public. Deadly computer viruses begin to infect computers in the United States, including many military systems. More than one million computers are affected, costing billions of dollars [38]. China media's broadcast of an exposed corpse of a U.S. soldier in the street of Iraq shake the determination of the Americans to act as the world's policeman. The intent of these attacks is also to influence the behavior of the American people and their government. These would not only be information warfare but also information operations.

In the real world, China looks for alternative methods such as IW to attack the United States. The cyber-world provides the simplest and quickest alternative to traditional physical attacks. The motives of cyber attacks are the same as a physical

attack such as a fighter plane launching a missile: to destroy a target. They generally seek financial gain, disruption, decreased military capability, fear/panic, publicity and news impact, decreased confidence in critical infrastructures/psychological operations, great physical damage, and even loss of life. Cyber attacks, whether stand-alone or coordinated, occur at the time and choosing of the adversary. They are inherently stealthy and can be used at critical periods.

3. Recent Examples of Information Attacks against the United States

Greek mythology features one well-known creative military idea, using the gift of a huge wooden horse that is hollowed out and filled with soldiers to infiltrate the enemy camp. Thus, the Greeks were able to avoid Troy's strong defense force and attack from the inside. Now the United States faces a similar condition. China has been attacking the U.S. Department of Defense's internal network in an attempt to bypass the United State's nearly impenetrable defenses and attack from the inside [71].

China is not only trying to purchase U.S. corporations, such as the IBM PC division, on the open market but is also stealing industrial secrets by taking over their computers. The latest attack, "Trojan horse," inserted a malicious code, named Myfip, into a company's network system to steal private information from compromised PCs. At least eleven other versions of Myfip, via spam, are searching sensitive documents such as CAD/CAM files used for mechanical analyses and design, and electronic circuit-board schematics and layouts. Once a user clicks on the included attachment, it will explore the internal network system to dig out specific files. Joseph Stewart, a senior computer-security researcher at Myrtle Beach, reverse engineered the Myfip code he received from customers. He discovered that Myfip was sending stolen information to an Internet user in Tianjin, China's third-largest city and second-largest hub for electronics manufacturing. Some Internet protocol addresses were connected to an Internet domain name registered in the name Si Wen in Tianjin. Stewart firmly believes that Myfip is just the beginning of a wave of China-support IW attacks intended to discover crucial trade secrets of U.S. companies [50].

Another obvious cyber-attack launched from China on the United States involved a group of Chinese computer hackers, code-named Titan Rain, which has successfully broken into U.S. computers containing top-secret information. Their method is to

commandeer a hidden section of a hard drive, zip up as many files as possible, and immediately transmit data to workstations in South Korea, Hong Kong, or Taiwan before sending them to mainland China. They always made a silent escape, wiping their electronic fingerprints clean and leaving behind an almost undetectable sign allowing them to re-enter the computer systems in the future. The whole attack process takes about ten to thirty minutes. Titan Rain, the router in Guangdong, China, is thought to rank among the most pervasive cyber-espionage threats that U.S. computer networks have ever faced. *Time* magazine has also obtained documents showing this kind of attack on facilities ranging from the Redstone Arsenal (home to the Army Aviation and Missile Command) to the World Bank [84].

The Department of Defense operates 3.5 million personal computers, including workstations and servers, and local-area networks (LAN) at 15,000 sites in sixty-five countries. It runs thousands of applications on thirty-five major voice, video, and data networks, including the nonclassified IP router network, which is connected to the Internet (World Wide Web), and the secret IP router network, which, following a physical separation strategy does not connect to the Internet. Though the networks provide commanders with timely combat information to make final decisions that play a critical role in the win-or-lose world of combat, they also represent a key vulnerability of the United States [38].

Internal U.S. Department of Defense networks and civilian companies' private networks are the Achilles' heel of the powerful U.S. giant. Securing networks is even more important than advanced weapons systems, such as tanks, destroyers, and fighter planes. Retired U.S. army officers and industry officials say that most of the hackers come from China, and the DoD's computer-network defense strategy is a war of attribution in which neither side has an advantage, because China is very aggressively developing this kind of capability [38]. Furthermore, the DoD's internal networks have been successfully penetrated and probed by China's hackers during the last five years. Outside hackers using Trojan-horse computer programs can operate within an institute's internal networks to reduce the computer systems' operational effectiveness and efficiency or steal invisible information that could result in huge damage in the future at practically no cost to themselves. Statistically, in 2004, there were approximately 74,053

attacks on military networks. This attack trend has continued to grow since 1997, when China honed in on this perceived drawback to U.S. network systems [34].

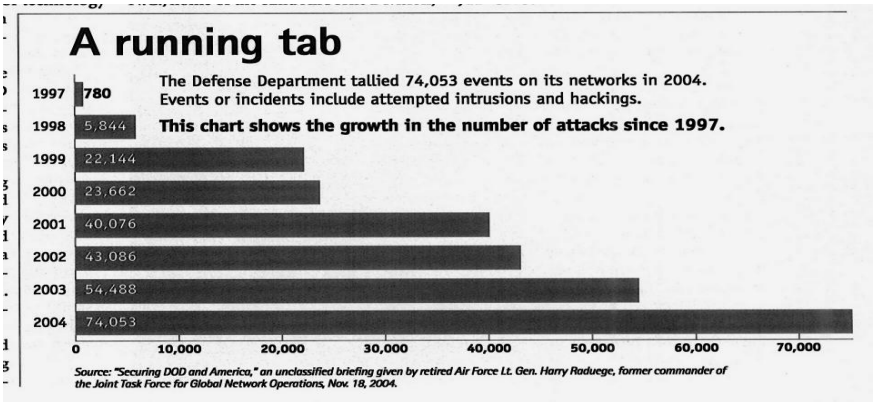

Figure 9. The Statistics about U.S. Network Attack (From: Frank Tiboni, "The New Trojan War," *Federal Computer Week*, August 22, 2005).

In keeping with China's evolving information-warfare strategy, Chinese hackers have used current advanced technology to conduct many, many intrusions focused on the United States. In one intrusion, China's hackers used a Trojan horse virus containing a malicious code to collect information via email about a future army command and control system. Hacking, or similar intrusions, happens at U.S. Army bases, too. These breaches caused the services to spend tens of millions of dollars to rebuild networks. In some incidents, hackers penetrated systems at Fort Campbell, Kentucky, home of the 101st Airborne Division; Fort Bragg, North Carolina, home of the 82nd Airborne Division; and Fort Hood, Texas, home of the 4th Infantry Division. Those intrusions provoked a serious response from the Department of Defense. One of the military's suggestions for enhancing its military networks is to establish simulated nonrealistic networks called "Honey pots." These can divert and trap China's attackers away from crucial computer systems and analyze their actions. Computer engineers can then use that information to patch an original system's weaknesses and create, in effect, counter-information warfare by the United States that has, itself, an asymmetric character [34].

Although a DoD official believe improved network management and vigilance would prevent 90 percent of the hackers' attacks, 10 percent would probably still occur,

because the threat from hackers has become so aggressive and sophisticated, and China's hackers use new knowledge to create new intrusion methods [38].

4. China's Information Warfare Force Deployment

Electrons and information technology are the foundation of the new twenty-first-century armed forces in China. Using IW capability as an asymmetric weapon requires operational effectiveness and efficiency, instead of concentration on pure military strength. Clouds of electrons or computer viruses would be able to disable and destroy a whole country. Thus, building systems for signal deception or interference will become as crucial as firepower [36].

On January 7, 2001, the Chengdu Company, the Sichuan Zhongcheng Network Development Corporation, and other companies cooperated to establish China's C-Net Strategic Alliance. The C-Net is a second-generation Internet-like network for the Chinese government and Chinese industries. According to a Xinhua News Agency article, "the current internet has too many faults and is incapable of satisfying the needs of the Chinese government and companies as they enter the digital age. It is unknown whether foreigners will have access to the net, or if it will be compatible with the existing net." [36]. Moreover, China's military communications system is carried over multiple transmission lines to make it survivable, secure, flexible, mobile, and less vulnerable to exploitation, destruction, and electronic attack.

China is now also considering the development of an independent "net force" branch of service to supplement its navy, air force, army, and Second Artillery Corps and to apply the thirty-six stratagems of war to its information warfare methods. China has placed an unusual emphasis on the emerging role of new IW forces. These various groups include a net force, a shock brigade of network warriors, information protection troops, an information corps, electronic police, and a united network People's War organ. The latter is worthy of the most consideration due to its unique nature and potential, for example, the existence of countless Chinese computer experts to participate in take-home battles [69].

A “net force “if developed would protect net sovereignty and engage in net warfare, a technology-intensive type of warfare. Net technology would include as follows.

Net technology	Purpose
Scanning technology	Break passwords and steal data
Superior offensive technology	Capable of launching attacks and countermeasures on a network, including information-paralyzing software, information-blocking software, and information-deception software
Masquerade technology	Capable of stealing authority from a network by assuming a false identity
Defense technology	Can ward off attacks, serve as an electronic gate to prevent internal leaks, and block arbitrary actions, much like an electronic policeman

Table 6. Type of Net Technology.

China has a number of superior software programmers and China’s Internet population has experienced explosive growth. The best industry publications estimate that, in barely three years from 1997 to 2000, China’s online population had increased from 200,000 to 16.9 million, making China one of the largest and fastest-growing “Internet countries” [7]. Ideas for uniting a People’s War with Information Warfare are finding fertile ground in the 1.5 million-reserve force of China. The PLA’s reserve-officer selection program also sponsors the college education of students and offers to repay their loans after graduation in return for a military service commitment. Kyna Rubin said that about 26,500 students, who in the past have studied in the United States[65] and now remain in China, studying in the following technological fields: instrumentation; computer-, electronic-, and microelectronic electrical systems; infrared and laser systems; radar; command-and-control, communication, computer, and intelligence-surveillance-and- reconnaissance (C4ISR) systems; identification and navigation systems; flight control; target acquisition; fire control; ECM/EW systems; IW; all-weather systems; fly-by-wire, fly-by-light, and active control; flight data recording;

training simulation; and air traffic control (ATC). These students, the best and brightest elite, will enhance China's overall information technology capability and also establish a strong foundation for its information warfare capability.

The People's Armed Forces Department (PAFD) organized twenty city departments — power, finance, television, medical, etc. — into a militia or reserve IW regiment. The PAFD has a network warfare battalion, as well as electronic warfare (EW), intelligence, and psychological warfare (PSYWAR) battalions, and thirty-five technical *"Fenduis,"* squad to battalion units. Several IW reserve forces have already been formed in the cities of Datong, Xiamen, Shanghai, Echeng, and Xian. Each is developing its own specialty as well.

The district of Echeng has reserve or militia units whose focus is conducting IW training. Shanghai reserve forces focus on advanced mobile wireless telecom networks and double-encryption passwords. The Xiamen area is a special economic zone that attracts a higher-than-usual number of science and technology clients; thus it is a prime area for IW-related activities. The Xiamen reserve forces conduct electronic countermeasures, network attack and defense operations, and radar reconnaissance operations. Datong *Fenduis* have conducted three opposing-force (OPFOR) demonstrations for the Beijing Military Region and General Staff. Xian *Fenduis* serve as OPFOR operatives for the Jinan Military Region; the unit uses ten IW methods as followed [37]:

1. Planting information "mines"
2. Conducting information reconnaissance
3. Changing network data
4. Releasing information "bombs"
5. Dumping information garbage
6. Disseminating propaganda
7. Applying information deception
8. Releasing clone information
9. Organizing information defense
10. Establishing network spy stations

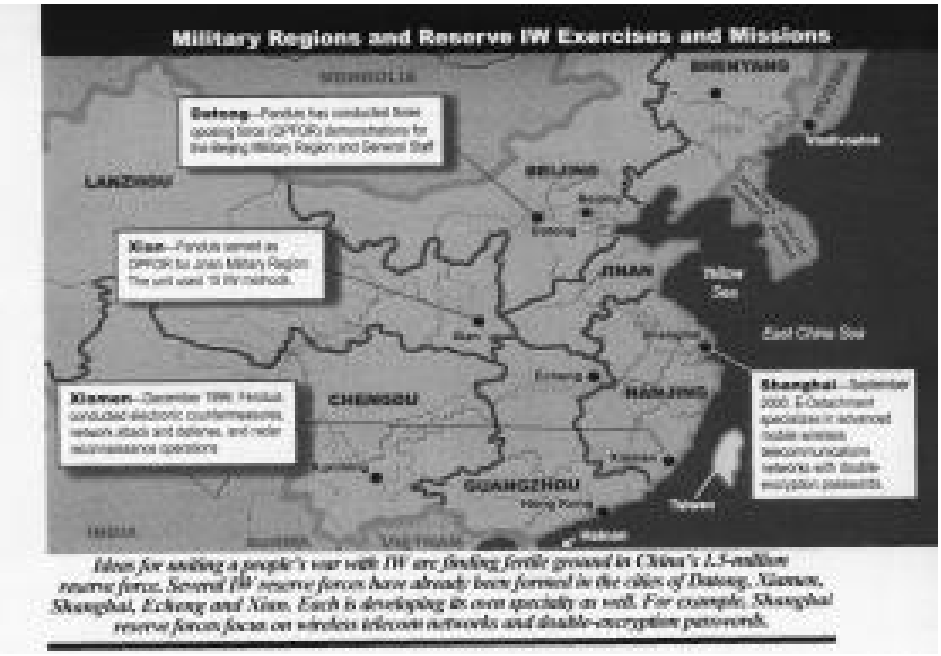

Figure 10. Military Regions and Reserves IW Exercises and Missions (From: Timothy L Thomas, "China's Electronic Strategies," *Military Review* (May/Jun 2001)**.**

The original role of China's 1.5 million-reserve force in a People's War was to support PLA forces defending against outside threats. Today's 1.5-million reserve force has a significant IW/IO mission and therefore has become the high-tech link in China's People's War theory. The reserve force can also do something that even the PLA could not for many years — "reach out and touch someone" continents away with electronic and information weapons. Properly targeted network attacks could be as devastating to a country's economy as damage inflicted by an intercontinental missile [36].

5. China's Information Warfare Exercises

Recently, China has conducted several important IW exercises that demonstrate the PLA's transition from theory to practice.

The first exercise was in October 1997 in China's Shenyan Military Region. A computer attack was launched that targeted a PLA group army and paralyzed its systems. The exercise, called an "invasion and anti-invasion" event, involved the deployment of ground, logistics, medical, and air force units.

A second exercise took place in October 1998 in China's Beijing Military Regions. This was an integrated high-tech exercise that used a "military information superhighway" — an information-network encryption subsystem of the command automation system, composed of digital, dial, and command net and restricted channels with transmitted graphics, characters, and audio data and situation maps.

The third exercise in October 1999 was also in China's Beijing Military Regions. Two group armies conducted a computer confrontation campaign on the network, including reconnaissance and counter-reconnaissance, interference and counter-interference, and blocking and anti-blocking practices. Also, a computer evaluation system analyzed the performance of the participants in a quantitative and qualitative manner.

Finally, a fourth exercise was conducted in July 2000 in the Chengdu Military Region. It was a computer confrontation campaign exercise on the Internet that included striving for air and information control and making and countering breakthroughs over a hundred terminals linked for the exercise. The number of IW military exercises conducted by the PLA continues to increase as the PLA continues to enhance its overall IW capabilities [69].

C. ELECTRONIC WARFARE

Electronic warfare (EW) is a military action that involves the use of electromagnetic and direct energy to control an enemy's electromagnetic spectrum or to attack the enemy by, for example, suppressing its air defense systems.

Regarding the use of NATO electronic warfare during the conflict in Kosovo, Serbia, Colonel Wang Baocun, a well-respected author on IO/IW subjects, describes how NATO worked first to behead the Serbian command and control (C2) systems, assuming the China old military strategy" Take the head and the body will follow." Wang emphasizes how Serbia's inferior armed forces, through a skillful use of defensive concepts, successfully thwarted NATO's superior armed forces' attacks [44].

1. They hid personnel and armaments to conserve their strength. They put aircraft in man-made caves; hid tanks in the woods, beside large buildings, or on mountainsides; separated the ground forces into individual villages

to mix with the Albanians; and transferred their command center underground.

2. Serbia's armed forces used their technical means successfully to avoid enemy detection: by not switching on their air defense radar, or only switching it on infrequently; by receiving coordinates and operational orbits from reconnaissance satellites; by switching off engines, putting equipment close to other heat sources, or putting fake heat sources in mock-up tanks; and by taking advantage of weaknesses in electronic surveillance equipment, for example, the fact that some systems don't operate if targets don't move.

3. Serbia also had ordinary people use the Internet, not to communicate with the outside world, but to hack into or overload NATO email servers. Thus, the Serbs conducted successful information operations — using information to influence the behavior of the United States and its allies. And they did this with relatively weak technology.

NATO's point of views was that it would destroy Serbia's air defense systems, leaving the skies relatively free of threats. Serbia, however, used a form of "guerrilla" warfare in which the air defenses refused to expose themselves, either physically or electronically. That made life difficult for NATO's air forces, and, as a result, NATO had to rely heavily on anti-electronic-warfare escort aircraft, especially the EA-6B, sent to the region.

At the time, Serbia was famous for having sophisticated air defense and command and control systems. Thus, U.S. and NATO operations against Serbia involved a wide variety of plans and ideas for coping with, disrupting, and disabling those systems. Initially, NATO attacked Serbia's basic infrastructure networks. By depriving large areas of electronic power and destroying communication lines and nodes, it forced the military and government to communicate via cell-phone systems, making their conversations vulnerable to Western eavesdropping [46].

The Washington-based Center for Strategic and Budgetary Assessments listed electronic warfare as one of the big winners in the Serbia–Kosovo conflict [47]. From observing that NATO operation, the Chinese PLA realized the importance of electromagnetic jamming, deception, compatibility, and pulse-bombs in causing the enemy's electronic equipment to malfunction: electronic warfare became the fourth dimension of the PLA's ground, naval, and air combat strategy.

Recently, in evaluating its electronic warfare capability, China emphasized the need to cooperate with Western companies. Using modern Western military technology and advanced design as a template, China is developing methods of reverse-engineering to improve its own EW and anti-EW weaponry systems. China has made progress in its development of RF weaponry as an air defense tool. RF weaponry disrupts the guidance and other electronic devices of cruise missiles and aircraft attacking a target. China is considering working with Russia to support China's research and development of a high-powered microwave system, referred to as Ranet-E, which would target the electronics on board precision-guided weapons [52]. China is also trying to procure state-of-the-art intercept, direction finding, and jamming equipment to upgrade its poorly equipped ground-based, ship-based, and airborne forces. In doing so, China has established close commercial ties with electronic companies in numerous foreign countries. Recently, an 11-76 cargo-transport aircraft arrived in Israel to be equipped with the EL-2075 Phalcon airborne-early-warning (AEW) system produced by System Ltd., Haifa, for use by China's PLA air force [32].

For the PLA, electronic warfare is as important as information dominance. The basic purpose of the PLA in conducting an EW attack would be to paralyze the enemy's integrated air alarm and air defense systems while also hiding an ongoing PLA military operation.

An advanced EW capability would allow China to conduct network surveillance and collect information on the performance, purpose, and structure of an enemy's military and civilian computer-information systems related to C4ISR, EW, and weapons systems. In addition, it could conduct electromagnetic surveillance for collection, positioning, inspection, recognition, recording, and analysis of electromagnetic signals from the enemy's electronic systems, and steal information via the electromagnetic spectrum [70].

D. CHINA: A "BIG" INFORMATION TECHNOLOGY AND INFORMATION WARFARE COUNTRY

China learned a lot about IT and IW from the battlefield performance of U.S. forces in Bosnia, Kosovo, Afghanistan, and the 1991 Persian Gulf War. And China now knows that advanced IT systems are the heart of many modern C2 systems. It is

continuously trying, therefore, to harness science and technology to develop an extensive dual-use information technology infrastructure. In doing so, China could improve its overall military capability. China has also made information technology and information warfare its highest military modernization priorities.

In his article, “China's technology stratagems,” Tim Thomas states that information warfare, defined as “knowledge-style warfare,” focuses on highly talented people with strong psychological qualities, command ability, and operational skills. In their implementation of that idea, the PLA leadership has decided to conduct IW training at different levels and according to different “categories” throughout its military force [44].

Their first category is support-style talent, with an age requirement of “over 40.” These people are designated as “decision-makers,” and the PLA’s overall goal with this group is to eliminate their information illiteracy. Their information training, which includes information technology basics, the theory of IW, and a general knowledge of IW weapons, is intended to change their concepts of traditional warfare and provide them with new ideas about future wars.

A second category is transitional-style talent, with an age requirement of “from 30 to 40.” As the future military leaders of China, they must concentrate on enhancing their ability to command and control in IW environments.

The third category is regeneration-style talent, with an age requirement of “under 30.” These people are familiar with information society and have an all-around foundation in modern information technology.

The IW training-for-individuals category covers a wide variety of knowledge, including computer basics and application, communications network technology, digitized devices, electronic countermeasures, radar technology, IW rules and regulations, IW strategy and tactics, strategic IW information systems, and information weapons. Especially strategic IW information systems include information gathering, handling, disseminating, monitoring, and using information in combat-decision support systems for command and control. Training in information weapons includes concepts of software-program and hardware-equipment destruction and ways to use these weapons to

conduct computer-virus attacks, to protect ones own information systems, and to jam the enemy's communication systems [69].

There are currently two hundred research parks and advanced-technology business incubators in China investing enormous energy into moving China's information technology development forward. Modern communication, data-links, and digitized systems are implemented by China's own massive research and development effort combined with large influxes of advanced foreign technology transfers. China export of IT products increased by 43.5 percent in 1999, and China manufactured 2.08 million personal computers, more than doubling the amount in the same period the previous year. During 1999, official statistics indicate that China produced 4.15 billion integrated circuits (IC), a 12.6 percent increase over 1998; 47.26 million program-controlled switchboards (PCB), a 53.6 percent increase over 1998; and 32.03 million mobile telecommunication facilities, a 44.6 percent increase over 1998.

According to the Minister of Information Industry, Wu Jichuan, China's overall IT sector will have an annual growth rate of 20 percent over the next decade and three times the projected growth rate for the national GDP. With significant support from the United States, China will become the world's second-largest IT market and is moving toward being increasingly self-sufficient in many related areas, including avionics; instrumentation; computers; electronics and microelectronics; electrical systems; infrared and laser systems; radar; command, control, communications, and computer intelligence surveillance and reconnaissance (C4ISR) capabilities systems; identification and navigation systems; flight control; target acquisition; fire control; ECM/EW systems; IW; all-weather systems; fly-by-wire, fly-by-light, and active control; flight data recording; training simulation; and air traffic control (ATC) [63].

In keeping with its significant growth in information technology, China is fielding a new generation of precise ballistic missiles guided by global positioning systems. China is also working on improving its space technology, including intelligence-gathering and satellite communications and navigation. It is also believed to be developing a ground-based laser anti-satellite system [62].

Given the host of skilled and smart mathematicians who currently reside and work in China, before long China's software and hardware programmers will no doubt develop creative and stable programs to guide and direct a Chinese long-distance cruise missile or a new version of a Trojan horse program capable of attacking U.S. assets.

E. SUMMARY

From 1985 to 2000, students from Asia's four main countries — China, Taiwan, India, and South Korea — earned more than 50 percent of the science and engineering doctoral degrees awarded to foreign students in the United States, four times more than students from Europe. More specifically, from 1985 to 2000, students from China earned, cumulatively, more than 26,500 science and engineering doctoral degrees at U.S. universities [81]. Huang Xinbai, a full-time member of China's state Education Commission in charge of sending Chinese students abroad, stated that sending students to study abroad is "a long-standing policy which remains unchanged and will never change."[80] He also indicated that many of the Chinese students sent to the United States were either state-funded or financed by various institutions and departments, based on China's needs.

Those students have a duty and responsibility to come back on schedule to serve their country when they finish their studies. Huang stressed that "they must put the interest of the nation first" [79].In his book, Red Dragon Rising, Triplett says that the PLA also uses Chinese students trained at American universities for the military field [80].

In some sense, the United States is training a future, though significant, army of Chinese information warriors.

V. FACTORS THAT TRIGGERED THE PLA TO PURSUE AN ASYMMETRIC WARFARE CAPABILITY

A. THE GULF WAR WAKE-UP CALL

It was not until the 1991 Persian Gulf War that the decisive role of modern information technology in warfare became indisputably clear. In another marked example, the 1999 NATO military campaign, the Pentagon successfully launched a cyberattack against Serbia. The impressive U.S. advanced-force demonstration revealed that a direct military confrontation with the United States would probably end up a failure. The United States' effective and efficient use of information and electronic warfare during the Gulf War and in Serbia inspired many countries, including China, to study and develop IW tactics such as computer network attacks (CAN) and EW tactics such as tactical reconnaissance conducted by China-made UAVs, in an effort to counter U.S. force and to explore ways to gain an asymmetric advantage over the United States [2].

Since much of Iraq's equipment was made by China and the coalition forces pummeled the Iraqi military, China realized its "modern" technology would not withstand a first wave of U.S. attacks in an open conflict. The PLA took notice not only of the United States' superior military technology — precision-guided bombs, stealth technology, airborne command-and-control systems, space-based intelligence, early-warning systems, and real-time C4ISR capability — but also of the destructive power of U.S. joint operations, created through the "synergy" of multi-service actions. The U.S. joint operations included simultaneous and coordinated attacks from air force fighter planes, navy strike missiles, and army helicopters. Such operations blinded, deafened, and quickly destroyed the opposing force's operation of a communications center and overall command-and-control systems to disable the enemy's further military action.

The PLA then understood that both its mass of traditional ground forces and its military doctrines were likely rendered obsolete. In addition, the demise of the Soviet Union, the end of the Cold War, and China's double-digit economic growth in the 1990s have allowed it to substantially increase it military spending on all the forces, army, navy, air force, and Second Artillery Corps. Because today's land and sea battles cannot be won

without integrative support from all the services, China purchased advanced weaponry systems from foreign countries, especially Russia. Thus, the PLA shifted its military strategy to one of force projection to defend the country beyond China's borders and incorporated the advanced weaponry necessary for fighting a "limited war under high-tech conditions" [7]. In fact, modern information technology has become the PLA's most important priority.

Thus, the Gulf War not only served as a catalyst for the PLA's development of information warfare to secure its position as Asia's "giant," but also as a marked signal that China must completely change the way its military is structured.

B. THE THEORY OF ASYMMETRIC CONFLICT

The boxer Muhammad Ali had a slightly faster punch and was lighter than his adversary, George Foreman. But no one thought that Ali could defeat Foreman in the World Heavyweight Championship fight of October 30, 1974 because none of Foreman's adversaries had lasted more than three rounds in the ring. George Foreman was not only the strongest but also the hardest hitting of his generation of boxers. At the fight, however, Ali made Foreman lose his temper by jibing at him: "George, you did not hit me"; "George, you disappoint me." That asymmetric strategy as initiated by Ali was completely successful. Foreman's punches became a furious blur; he was completely confident that no one could bear his heavy hits. As he hit Ali again and again, Ali appeared to cower against the ropes. But the elastic ropes were actually absorbing much of the force of Foreman's heavy hits: Ali was simply waiting for his chance as Foreman wore himself out. Finally, in round eight, Ali knocked Foreman out and the fight was over. Foreman's prodigious punches proved useless against Ali's rope-a-dope strategy, resulting in a fight outcome that was totally unexpected. Ali's fight strategy illustrates an important aspect of asymmetric warfare and how a weaker country like China could defeat a strong country like America [72].

The idea of a weaker country defeating a strong country (The stratagem of Sun Tzu "using the inferior to defeat the superior") is a well-known way of thinking for Western scholars. For instance, in Thazha V. Paul's research comparing six cases of war initiated by weaker countries, he studied the dynamic of asymmetric conflicts [54]. And in an interesting article, "How the Weak Win the War," published in 2001, Ivan

Arreguin-Toft examines the circumstances under which a weaker country (refer to weaker military strength) actually defeats a stronger country (refer to stronger military strength). Using statistical and in-depth historical analyses of armed conflict spanning two hundred years, Arreguin-Toft breaks the time span into four fifty-year segments. His research shows that, among all the asymmetric conflicts in the 1800–1998 periods, the stronger countries won 70.8 percent of the time, the weaker countries won 29.2 percent of the time. Moreover, he finds evidence showing that the nineteenth century favored the stronger countries in asymmetric conflicts, with the weaker countries winning only 11.8 percent of the time for 1800–49 and 20.5 percent for 1850–99. But weaker nations that simply try to defend their territory, such as in the Iraqi insurgency, may actually enjoy a significant advantage over a larger opponent, which is bound to a larger degree by world opinion and the limits of its own war methodology.

However, the more interesting discoveries in Arreguin-Toft's study show that the weaker countries won a gradually increasing percentage of asymmetric conflicts (for example, weaker country North Vietnam traditional guerrilla operation resolved the fighting will of stronger country U.S. ,which used lots of advance fighters for heavy bombing operation) over time. That is, evidence from the twentieth century indicates that the weaker countries got a much better chance to overcome the stronger one during the later periods. They won 34.9 percent of all asymmetric conflicts for the period 1900–49 and 55 percent for 1950–98. Thus, in the latter half of the twentieth century, not only were the weaker countries more prone to initiating the wars than in previous periods, but also they were more likely to win. A good example of this is the Vietnam War from 1954 to 1975, an armed conflict between a weaker country, North Vietnam, and a stronger country, the United States.

Arreguin-Toft's overall finding challenges the traditional concept that military strength is the dominant factor on the battlefield, that the stronger country always has a better chance of winning than the weaker country. These findings should be of considerable interest to countries like China [54].

Ivan Arreguin-Toft continues by analyzing the various scenarios within which strong countries can be defeated by their weaker counterparts. He refers to the thinking of

Mao Zedong that, when a weaker country conflicts with a strong one, the weaker will benefit from certain interactions of direct- and indirect-approach strategies. For example, historically, the Chinese Communist Party (CCP) has exploited its opponents' weaknesses, using asymmetric strategies against a better-funded and better-equipped opponent (KMT). For instance, a CCP propaganda war successfully stigmatized the KMT as the enemy of all groups in China, poor and rich, peasant and bourgeois.

Arreguin-Toft defines "direct" approaches as those aimed at destroying an adversary's *ability* to fight, whereas "indirect" approaches aim to destroy the adversary's *will* to fight. He postulates that, when a stronger one attacks with a direct strategy and the weaker one defends with an indirect strategy, the weaker one will win. Conversely, when an attack occurs in which a stronger country uses an indirect strategy and the weak one uses a direct strategy, the weak one will also win. Arreguin-Toft sums up the expected effects of strategic approaches on conflict consequence in a matrix, with the expected winners identified in the cells of the matrix.

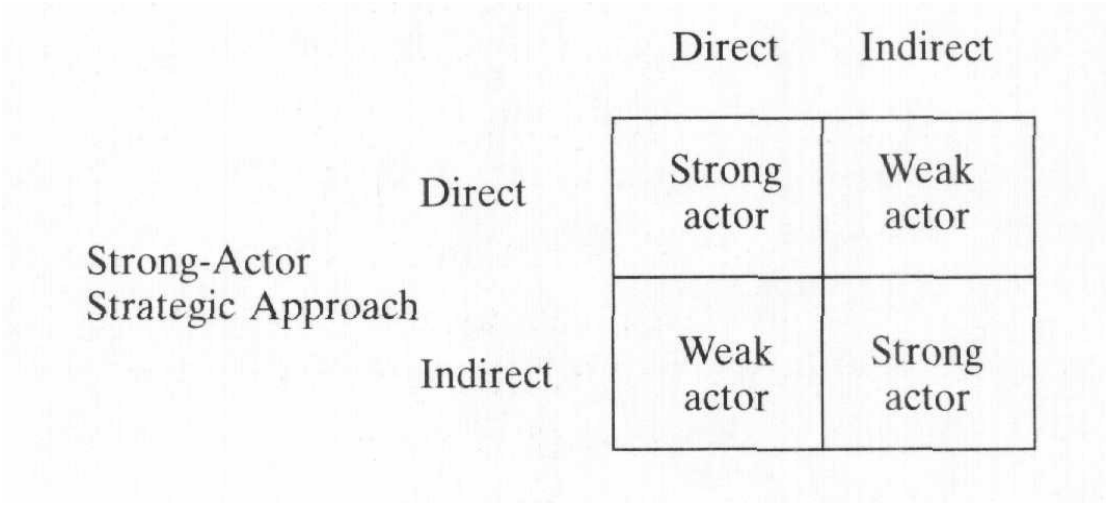

Figure 11. "How the Weak Win the Wars" (After: Arreguin Toft, 2001).

In brief, the interaction of *similar* strategic approaches favors the stronger adversary, while the interaction of *dissimilar* strategic approaches favors the weaker one. This new perspective on asymmetric conflicts allows us to makes sense of how the United States was able to win its war in Afghanistan (2002) in just a few months, while the Soviet Union lost its war there after a decade of brutal war (1979–1989).

In Arreguin-Toft's "How the Weak Win Wars," he used expert scholarly analysis to support the idea that strategy is most important when a stronger country faces a weaker country in asymmetric armed conflict. The probability of victory or defeat in such conflicts depends on the interaction of the strategies that the weak and strong countries deploy. His work also points out the serious consequences of ignoring the importance of that strategic interaction. All these ideas illuminate and support China's decision to pursue an asymmetric-warfare strategy and serve as a warning to U.S. policy-makers to get their military strategy right, regardless of their relatively greater power [54].

C. SUN TZU'S STRATAGEMS

Historically, the so-called Warring States period in Chinese History began when seven major states that are shifting alliances and slow consolidation resulted in the first unification of China under the Qin state. Sun Tzu, a military leader for one of the warring states, who led troops with brass-tipped spears and rhinoceros-hide shields, was and also determined to record his strategic and tactical record for later generations. His work has not only continued to affect China's military writing but also helped guide the high-tech warfare in the Persian Gulf. The Iraqi military used fake fiberglass tanks and aircraft to trick the allies into wasting million-dollar missiles on useless target. Saddam's Scud missile attacks on Israel, aimed at drawing Israel into the war and unraveling the anti-Iraq coalition, fit in with Sun Tzu's advice: "If the enemy has no alliance, the problem is minor and the enemy is weak."

Sun Tzu, a figure of sixth-century B.C. China, preached a military philosophy of subtlety and cunning in a tiny book called "The Art of War." This book has stirred new interest among the Chinese and contributed to a revolution in basic tactics in its armed forces. "You could say Sun Tzu's spirit is hovering above the whole conflict," said Colonel Sam Gardiner, a retired air force officer who used to head an information security department at the National War College in Washington [67].

Sun Tzu's thinking was the opposite of the thinking of people in the U.S. military who argue that massive firepower is the dominant factor on the battlefield. Rather than applying massive firepower, Sun Tzu argued, the successful military leader will outwit his opponent by military preplanning, psychology operations, information-gathering,

deception, surprise, ambushes, rapid thrusts through enemy lines, and any other methods that will throw the opponent off balance and attain a desired goal at a minimal cost.

Sun Tzu's works, assembled as "The Art of War," reached the Western world in the late eighteenth century, when they were followed by the Soviet Red Army and the Japanese military. Sun Tzu's admirers stretch back through history. They include China's revolutionary leader Mao Zedong, Vietnamese guerrilla leader Ho Chi Minh, and Napoleon, the Emperor of France [68].

There was a lot of Sun Tzu in the tactics that allowed the North Vietnamese forces to overcome superior U.S. weapons systems. A standard North Vietnamese tactic was to initiate an attack with mortar cover, then infiltrate a small band of troops behind U.S. lines to sow confusion and strike from the rear. This military action followed precisely Sun Tzu's suggestion about seizing the enemy's attention with the application of an ordinary force, then knocking him off balance with an extraordinary force. A couple of Vietnamese soldiers could do a huge amount of damage to traditional U.S. military forces, because no one would know where they were and or what they were doing. Such swift thrusts and retreats often proved far more effective and efficient in hurting the enemy than did massive firepower.

In a war in which the Americans often struggled to understand the Vietnamese, the North Vietnamese seemed to succeed by following Sun Tzu's suggestions about understanding the psychology of your foes and friends and about fostering good relations with civilians.

Samuel B. Griffith, a retired Marine brigadier general who translated and published Sun Tzu's works, once wrote that "The *Art of War* should be required reading for those who hope to gain a further understanding of the grand strategy of the Chinese leadership" [68].

According to China's former leader, Deng Xiaoping, China's defense industry lags in the development of high-technology equipment; therefore, China must find "selective pockets of excellence" rather than attempting to match the United States's comprehensive power. Under the influence of Sun Tzu's concept of "overcoming the superior with the inferior," China's civilian scholars and military officers explored

China's potential for information and electronic warfare. They decided that China, as the weaker party, should use an asymmetric warfare capability, such as sending email computer viruses, in a modern war against a stronger but vulnerable adversary, such as America, thereby applying Sun Tzu's traditional stratagem: "Fool the emperor to cross the sea" [45].

The idea of asymmetric conflict challenges classic deterrence theory, which assumes that the status quo deters anti-status-quo power due to the former's dominant military strength. In the past, the PLA was able to compensate for its insufficient firepower or manpower with superior unconventional strategies, such as guerrilla warfare, psychological warfare, political propaganda, and a united front. The PLA reckons that, throughout its history, it has had to fight several stronger rivals: the KMT in the Chinese Civil War, the United States in the Korean War, and the USSR in the Sino-Soviet border war. So the concept of "overcoming the superior with the inferior" is deeply rooted in PLA strategic thinking. But now the PLA feels strongly that, in the twenty-first century, it must harness high technology in its struggle against its most probable and most powerful strategic rival, the United States. In developing IW/EW, the China still believes that superior strategies can help overcome technological deficiencies [2].

D. THE ARMS EMBARGO

Russia is one of China's main weapons sources. Over the past decade, Moscow sold Beijing more than 150 advanced fighter planes, two destroyers, and more than 1,000 various missiles, with ranges greater than the 160-kilometer-wide Taiwan Strait. In one ongoing deal, China will receive eight Kilo-class diesel-electric submarines from Russia to supplement the four China had previously purchased. Israel is another of China's weapons suppliers. In a 2001 Israeli transfer, China received HARPY unmanned aerial vehicles, and, in 2003 and 2004, Israel subsequently conducted maintenance on them. In China's military modernization, it purchases many advanced weapons from foreign countries and gets a good opportunity to improve its overall military capability. However, the current arms embargo may be driving China to pursue asymmetric techniques (Since 1989, the United States and the twenty-five-member European Union have prohibited the sale of weapons to China).

Although China announced that it spends about $20 billion annually on its military, the Pentagon contends that China spends about two or three times as much, possibly as much as $90 billion. This would rank China as Asia's biggest weapon buyer. However, Beijing has objected to previous U.S. estimates of China's military expenditures and states that the bulk of China's military expenditure is used for improving the living conditions of its military officials and soldiers. In contrast, the U.S. military report focuses on China's advanced weapons system purchases. In recent years, China also put an effort into the indigenous production of weapons and importation of fighter planes, destroyers, submarines, and various missiles.

The U.S. administration is afraid that those weapons might eventually be used against Taiwan, because China regards Taiwan as a rebellious province that should be brought under the mainland's control, either by military means or peaceful means. But the United States considers Taiwan as a buffer against a Chinese power expansion in Asia. Moreover, the United States has numerous interests in the Asian and Pacific region, including the security of Japan, Taiwan, South Korea, and the South China Sea. U.S. Armed forces, which are deployed throughout the region, could be jeopardized by China's modernized military force, because it is increasingly well armed and seeks to settle long-standing territorial and political disputes in the region by force.

China has already benefited from previous weapon sales, such as the British SPEY MK 202 engine used on its FB-7 bomber. Such an acceleration of China's military modernization could have a direct impact on stability in the South China Sea and the safety of the United States. It could accelerate a shift in the regional balance of power and affect the security of many other countries.

The United States bristles over its allies supplying China with weapons systems and related military technologies, by which China takes advantage of Western technology and manufacturing expertise to improve its indigenous industrial capability for the production of future weapons systems over the long run. Although, in the past, European companies have delivered military hardware to China, an attractive weapons-import market, they have not supplied any major weapons systems, such as advanced fighter aircraft, tanks, destroyers, or highly sensitive technology such as C4ISR (command,

control, communications, and computer intelligence surveillance and reconnaissance). There is no doubt that Europe's uncertainty and its hesitation to lift the arms embargo against China is due mostly to pressure from the United States. All the European allies clearly understand that Washington's reaction would most certainly not be limited to purely verbal protest, but would have a potentially devastating impact on the overall trans-Atlantic partnership [56].

The Bush administration is concerned that lifting the arms embargo would allow the Europeans to sell advanced technology to China, which would enable China to shift to "next generation" warfare capability and prompt China to further develop complex modern weaponry systems similar to those the United States has used in both the Afghanistan and the Iraq War. Those systems could cover highly sensitive C4ISR technology, advanced airborne radar and communication systems, and the American E-8C Joint Stars aircraft that assists a battle commander to direct troops and fast airstrikes on the battlefield [57]. In addition to rapping the European Union for assisting in China's military modernization, the United States also uses its influence on Israel for its cooperation with China. Recently, to reduce U.S. concerns, the Israeli administration stop the weapons sales to China.

On February 1, 2005, four members of the U.S. Congress, Mr. Hyde, Mr. Lantos, Ms. Rose-lehtinen, and Mr. McCotter, submitted the following resolution in the House of Representatives to urge the European to maintain its arms embargo on the People's Republic of China.

1. Reaffirms the United States arms embargo on the People's Republic of China.
2. The policies made by United States and other countries which promote the development of democracy in the People's Republic of China and not the development of China's military capabilities will help assure a stable, peaceful, and prosperous Asian and Pacific region.
3. Deplores the recent increase in arms sales by member countries of the European Union (EU) to the People's Republic of China.
4. The European Council's decision to finalize work toward lifting its arms embargo on the People's Republic of China is an action that places the European security policy in direct conflict with the United States' security interests and with the security interests of the United States' friends and allies in the Asian and Pacific region.

5. Declares that such a development in European security policy is inherently inconsistent with the concept of mutual security interests that lies at the heart of United States laws for transatlantic defense cooperation at both the governmental and industrial level and would be unwelcome on both sides of the Atlantic.

6. Requests the President in his forthcoming meeting with European leaders to urge that they reconsider this unwise course of action and, instead, work expeditiously to close any gaps in the European Union's arms embargo on the People's Republic of China, in the national export control systems of EU member states, and in the European Union (EU) Code of Conduct on Arms Export in order to prevent any future sale of arms or related technology to China.

7. Requests the President to inform Congress of the outcome of his discussions with European leaders on this subject and to keep Congress fully and currently informed of all developments in this regard [58].

China is not only behind the Western countries in developing a self-owned high-tech weaponry system, but also the United States and its European allies have put an arms embargo limitation on China. Although China has a strong appetite for European military defense technology in order to challenge the United State's firepower and its ability to coordinate its force (C4ISR), China still cannot receive enough military resources to compete with the superior military strength of the United States.

Does a single hacker attack count as a hostile act? Can using financial instruments to destroy a country's economy be seen as a battle? Did CNN's broadcast of an exposed corpse of a U.S. soldier in a street in Iraq shake the determination of the Americans to act as the world's policemen? Did terrorist attacks such as September 11th on the United States constitute a form of asymmetric warfare?

When we suddenly realized that these non-war actions may be the new factors constituting future warfare, a new name transcends all boundaries and limits — Unrestricted Warfare. Those factors, such as arms embargo limitation, forced China to pursue the asymmetric warfare capability to secure its dominant position in Asia and the world.

VI. IBM'S LENOVO DEAL INCREASES U.S. SECURITY FEARS

A. INTRODUCTION: THE CASE STUDY BACKGROUND

In 1981, IBM envisioned computing at a new level, a personal level, to extend the convenience, power, and productivity of information technology (IT) from the mainframe to the individual either at home or in the workplace. This action resulted in the establishment of a new unit within IBM, the Personal Computing Division (PCD), which focused completely on personal computing operation. The PCD advanced state-of-the-art technologies with a series of widely ranging innovations, from the very first Notebook to the latest high-security technologies. One of their security research and development projects involves a biometric identification system that protects a user's identity from invasion by hostile outsiders, or hackers.

In 1984, not long after the PCD was established, eleven computer engineers and researchers in Beijing, China, set up a company that brought the convenience, power, and productivity of information technology into the lives of millions of Chinese people. The computer company, Legend, not only introduced PCs into Asian households but also promoted PC use throughout China by establishing retail shops nationwide. The company also developed pioneering PC technology such as language translation for computer operating systems. Legend's Chinese Character Card translated English operating systems software into Chinese characters.

By 1994, Legend was trading on the Hong Kong Stock Exchange and four years later produced its one-millionth PC. In 2003, Legend changed its brand name to Lenovo; taking the "Le" from Legend to resound Asian heritage and adding "novo," the Latin word for "new" to reflect the spirit of innovation as the core value of this international company.

Lenovo holds more than a quarter of the market in China, where 15 million PCs were sold in 2004, second only to the United States. But with its market share unlikely to climb much farther in China, it has had to look beyond its home turf for future growth. Conversely, IBM has its own reasons for its retreat from the PC business. Although Big Blue (IBM) helped make PCs a global phenomenon, IBM now makes little profit from

PC sales. Despite the fact that PC sales grossed 11 billion U.S. dollars for IBM, it often loses money in the production of these units. With Lenovo's landmark acquisition of IBM's Personal Computing Division in May 2005, the new Lenovo will acquire IBM's entire global desktop and laptop computer research and development and IBM's worldwide distribution and sales network, resulting in a sales presence covering 160 countries.

Through this acquisition and Lenovo's links to the Chinese military and government agencies, they will own 30 percent of the global PC market share and IBM will own 15 percent. Lenovo will become the new global PC market leader with annual revenue of $12 billion [74]. However, the sale of IBM's PC business to Lenovo will also increase the potential for industrial espionage. The Chinese government owns a large stake of Lenovo, thus the likelihood in the transfer of technology for possible military use.

B. LENOVO HAS A STRONG CONNECTION WITH THE CHINESE MILITARY

China's domestic information technology industry is known to be developing IW-related tools. The Guangzhou Communications Research Institute is directly subordinate to the Ministry of Information Industry. It is engaged in the research and development of mobile communications systems and networks, including digital multi-path radio relay systems. Moreover, the China's domestic IT industries occasionally receive foreign assistance with their research and development. In 1997, the U.S. firm Hewlett Packard established a memorandum of understanding for collaboration with the Chinese Academy of Science's Information Security Technology and Engineering Research Center. This collaboration of efforts involves conducting research and development and the application of information security technology [78].

In fact, Lenovo was a state-owned business which received support from various Chinese government agencies including the PLA. According to the People's Daily Online, a Chinese Website, Lenovo released China's first security chip. The chip, Heng Zhi, is designed to maintain the stability of personal computer systems for verifying PC identification and establishing credibility for data exchange such as online shopping. Present regulations stipulate that security chips used by the Chinese government and the

military must be developed by local firms that do not use any foreign-developed technologies, material, or designs in the development of their chips [77].

C. CHINA'S GOVERNMENT PROVIDES FINANCIAL SUPPORT FOR ACQUIRING U.S. CORPORATE ASSETS

"The past year saw Chinese firms bid to take control of three major U.S. companies," reported the U.S.-China Economic and Security Review Commission (USCC). One of those bids was the Lenovo Group's acquisition of the IBM Corporation's Personal Computing Division. Another such attempt is the Beijing-based Chinese National Offshore Oil Corporation (CNOOC), of which the Chinese government owns 70 percent, which tried to acquire an America oil company, Unocal, based in El Segundo, California. CNOOC's bid was $18.5 billion more than an earlier bid from Chevron. The move on Unocal generated significant opposition in the U.S. House of Representatives. The House urged President George W. Bush to instigate an overall review of the deal through the Committee on Foreign Investment in the United States (CFIUS), and the bid to purchase Unocal, the sixth-largest U.S. oil company, ended in failure. A third case was a $1.2 billion bid by the Chinese firm Haier for Maytag Electronics; this bid was usurped by a rival U.S. firm [75].

These U.S. corporate acquisitions and attempts at acquisition by Chinese firms signal the beginning of China's efforts to gain an asymmetric advantage over the United States. USCC is responsible for monitoring China's growing global economic influence and military might. In its annual report to Congress, the Commission reported that the Chinese government has amassed $769 billion in foreign reserves that state-sponsored companies such as Lenovo can spend on the acquisition of U.S. corporations. Now that China has money to purchase U.S. businesses like the icon IBM, it is creating shock and concern in Washington, D.C. This is because IBM's PC hardware and technology is ubiquitous in the lives of the U.S. populace. And there are some types of high-level software or specialized computer hardware that have a defense application and could enhance China's military by, for example, helping it better network its military assets.

On numerous occasions in the past, China's authoritarian regime has stated publicly that the United States is its ideological enemy. Comments made by China's Chen Yonglin to Australian authorities in June 2005, for instance, support the theory that

China's leaders view the United States as their main adversary. Therefore, the Lenovo Group's $1.75-billion purchase of IBM's PC business could well imperil U.S. national security. Thus, the U.S. Congress must block such deals in the future on the basis that China represents a strategic competitor and a threat to U.S. security [75].

D. CHINA'S NEW PC MARKET MAKES CYBER ATTACKS MORE POSSIBLE

China's Ministry of Information Industry statistics indicate that China had more than 20 million computers in 2000 and an electronic information network with a wideband that covered most Chinese cities. More than 34,000 Chinese companies have registered their domain names on the Internet. According to the Gartner Group, a global research firm, China is the world's second-largest PC market and is growing seven times as fast as the current volume leader, the United States. With 1.3 billion citizens, China will likely have 100 million computers in the next decade. The increasing availability of computer technology in China is a concern for the United States, which sees an intrusive and menacing Chinese government as the driving force behind the country's dramatic PC market growth; for example, China government helps Lenovo to buy IBM's PC division to secure its world PC market position.

"They are ignoring cyber security and it poses an enormous vulnerability," said Edward Lazowska, professor of computer science and engineering at the University of Washington.

Asia, especially China, is already the leading breeding ground for software piracy, hacking, and virus proliferation. Therefore, it is not difficult to imagine young groups of Chinese hackers feverishly at work in hundreds of government-sponsored hacking centers attacking U.S. government computer systems.

In 2001, hackers in China launched targeted attacks against U.S. websites in response to the death of a Chinese pilot killed in a collision with a U.S. spy aircraft. On May 1, 2001, the official Chinese government publication *People's Daily* claimed that 92 Web sites were under attack, including those of the Energy Committee and State Security of California. Ninety-two percent of the requests to the CIA's government Web site were unfulfilled because of a "denial of service" attack; the White House and U.S. House of Representatives sites were also shut down. By the morning of May 5, over 1,400 U.S.

sites were shut down by the Chinese hacker attacks [83]. Since then, the United States keeps a closer eye on China's information-warfare development, given that China's emerging PC market makes cyber attacks more possible than ever.

E. U.S. SECURITY WORRIES

China has long been a focus of deep concern for the Bush administration. The 2001 U.S. Quadrennial Defense Review (QDR), a key military planning document, notes that the United States "will not face a peer competitor in the near future." However, the QDR then highlights the possibility that "a military competitor with a formidable resource base will emerge" somewhere in the "East Asian littoral — from the Bay of Bengal to the Sea of Japan." This statement points indirectly to China, the world's most populous country. China has the world's largest standing army and, as a military authoritarian country, does not share U.S. democratic principles.

Moreover, China has made a number of below-the-surface formative decisions in the past, from weapons systems acquisitions to missile defense to the import of dual-use and military technology to access "missing pieces" of its military capability. Beyond Osama bin Laden, the ongoing military modernization in North Korea, Iran, and China, along with China's ambitions for Taiwan are among the prominent items on the United States's list of security worries [76].

The *Bloomberg News* and the *International Herald Tribune* both reported one of the terms in the Lenovo $1.75-billion IBM acquisition: IBM becomes a reseller for Lenovo's desktop and laptop PC clients. In addition, Lenovo gains access to IBM's contracts, including its vendor status with the U.S. General Service Administration for government computers. The concern of the U.S. government is that Lenovo is partly state-owned and thus could possibly be an arm of the Chinese military. This may not only result in technology with important military uses, such as the transfer of encryption technology, battery technology, and product integration being passed on to China, but also Chinese nationals working for Lenovo in the United States might act as industrial spies. The proximity of higher-end IBM operations research in Triangle Park, North Carolina, to the site Lenovo will buy could make industrial espionage easier. This

concern of U.S. officials is not new. The Chinese government has a long history of using business and cultural activities as fronts for espionage of all types in the United States [74].

The "national security" concerns surrounding the IBM deal are voiced by Michael Wessel, a member of the congressional panel that monitors Sino–U.S. transitions, the U.S.–China Economic and Security Review Commission. Wessel told the *Washington Post* that Chinese computer experts could conduct industrial espionage from IBM facilities. The modern advanced technology that Lenovo acquired in the deal could have a "dual use" and enhance the overall capability of the People's Liberation Army. Wessel made this comment based on what happened after the 1995 purchase by China companies of the Anderson, Indiana–based Magnequench, which makes railroad magnets used in the guidance system of smart bombs.

F. THE CONNECTION BETWEEN IBM AND U.S. MILITARY APPLICATIONS

The style of future warfare will be less dependent on the most physical assets such as warships, fighter aircraft, and tanks, but more determined by who has the best information and the most efficient means of sharing it among all elements of the fighting forces. In 2005, Boeing and IBM stated that they would join hands to develop ground- and space-based systems to enhance U.S. military communications, intelligence operations, and homeland security. This agreement created a strategic alliance, bringing together the second-largest U.S. defense contractor and the leader in information technology to address an estimated 200-billion-U.S.-dollar market [82]. IBM will provide Boeing with information management middleware and design elements for electronic systems products, integrate leading-edge technology into a variety of networking and computing systems, and provide microprocessor technology.

Lenovo's co-founder and chairman, Liu Chuanzi, who has a very close relationship with the PLA, came from a military background. Statements made by him that the company, Lenovo, is interested in increasing global sales remain open to healthy skepticism. Prior to the Lenovo sales, IBM's PC business had been losing approximately $1 billion dollars per year for the past several years. From a business standpoint, none of the companies with excellent vision is willing to take on this terrible business, except

Lenovo. The acquisition of IBM has the added China's asymmetric advantage of creating an interest group in countries that are economically dependent on China. Therefore, these countries will tend to be favorable to China's interests, such as improving China's information warfare capability.

G. SUMMARY

After the new Lenovo was formed, it would absorb the 1,900 American workers in IBM's personal computer business. Other Chinese companies, with their increasing wealth and global ambitions, are expected to follow Lenovo's example.

The West decided that the best way to deal with China is to increase commerce to encourage economic and political liberation. Why did the United States not make an effort to block IBM's sale of its personal computer business to Lenovo, China's largest computer maker? In the past, the United States has blocked sales to Chinese firms on similar grounds. In 2003, Global Crossing Ltd. failed to obtain approval from the committee to sell its telecommunications network to the Hong Kong–based Hutchison-Whampoa Ltd. Dealing with an authoritarian military country like China as it emerges as a great power is one of the most difficult issues in the United States today. It won't be any easier if the United States decides it is better off selling PCs to Beijing than selling advanced weapons.

A Chinese government agency, the Chinese Academy of Sciences, which owns a third of Lenovo, plays a key role in exploiting advanced technologies to enhance the PLA's military technology capability.

The purchase of IBM's PC division was eventually approved by CFIUS [78], but IBM's close ties with the largest Chinese PC maker could result in leaks of sensitive technologies. There is an old Chinese saying: "Businessmen have no mother country; their only focus is profit." Lenovo might transfer sensitive technology developed by IBM — such as innovation in nanotechnology or the science of making molecule-sized devices — to China's military. This type of technology would surely make the next generation of Chinese PCs more powerful than ever.

Due to its massive pool of cheap labor and its potential market, China's development strategy has been based on attracting foreign investment to China. The

intent was to build industries and acquire advanced technology. For example, most of the notebooks PCs were manufactured by Taiwan, but, in 2005, the latest notebook production line was moved into Chinese factories to avoid the expensive labor costs in Taiwan.

Various foreign, advanced dual-use information technologies is being transferred to China, particularly through Hong Kong and the surrounding Pearl Delta region with its various special economic zones. In the 1990s, China used advanced encryption devices from the United States to make its military codes more secure. It seems prudent to anticipate that such IT innovations will benefit China's IW capability. Since China started by simply acquiring IBM's PC research and development capability, such thinking seems quite plausible. With additional foreign research and development assistance, China could develop creative and stable computer-virus programs on its own. Such a result would certainly be against America's strategic interests.

VII. SUMMARY AND RECOMMENDATIONS

China, whose population represents about 20 percent of the world's 6.3 billion people and whose territory covers nearly 10 percent of the Earths surface, is a rising future star on the world stage. After China's excellent leader Deng discarded many of Mao's outdated policies and introduced economic reforms, China's booming economy has produced double-digit gains every year since the mid 1980s. This explosive growth raises the prospect of China emerging as a major global power. To help secure this potential new status, China determined to modernize its military to get position recognition in the world community and become militarily competitive with other global powers, especially the United States.

It is not surprising that China used both the rapid growth of the economy and its abounding natural resource to enhance its overall military capabilities. For the past two decades, the PLA has undergone a significant downsizing and conducted a series of military modernization actions to build a more effective and efficient PLA. Also, China has established a close relationship with Western countries' most-advanced industries in order to acquire their many state-of-the-art weapons systems. In addition, China's defense industries received high-tech weaponry systems indirectly from foreign countries in hopes of developing "reverse-engineering" capabilities to strengthen China's indigenous weapons production.

Thus, China, possessing one of the fastest growing economies in the world combined with one of the largest military machines, shows its ambition to achieve regional hegemony in Asia as well as a dominant position in the world, in addition to posing a threat to U.S. interests. However, China's economic reform has also slowed its military modernization efforts and hindered indigenous defense production. Chinese strategists, therefore, began to explore China's information-warfare potential in order to pursue an asymmetric warfare advantage. Following China's classic military strategist, Sun Tzu, two senior PLA colonels proposed "using the inferior to defeat the superior" and "winning the war without bloodshed."

In their book, *Unrestricted Warfare***,** Qiao Liang and Wang Xiangsui propose a series of asymmetric strategies for securing China's dominance as a global power. While technology may change the methods, China's traditional operational strategy remains the same: its techniques are still employable in the context of modern technologies and modern conflicts. For example, one of the China's ancient operational strategies—"Fool the emperor to cross the sea"—in today's world becomes the use of regular e-mail services, e-commerce, or e-business-links to mask insertions of malicious code or "backdoor" programs in order to detect weaknesses in U.S. military networks.

For China, information technologies provide asymmetric capabilities. While the definition of asymmetric warfare has changed over time, its basic concept — the use of unorthodox methods and capabilities to undercut enemy s strengths — remains the same. China has practiced asymmetric warfare for thousands of years in its long history, and it can be used now against the United States' superior military force and thereby avoids exposing the very limited power-projection capability of China's conventional military. The PLA can use asymmetric methods, such as computer network attacks, to delay and deny the United States' technologically advanced force by exploiting the United States' very reliance on that technology. This capability of computer network attacks could be enhanced through the IBM–Lenovo deal.

According to *Unrestricted Warfare,* the new principles of war indicate that using only armed forces to suppress an enemy is no longer recommended. It is much better and more efficient to use all means available, including armed forces and unarmed forces and military and nonmilitary means to suppress the enemy. These new war principles provide a great opportunity for China to topple the American hegemony. In facing the new style of future warfare employed by China, the United States must unify public support and strengthen the people's will to fight to defense against China's threat of asymmetric operations.

LIST OF REFERENCES

1. "China's Stealth War on the U.S." http://www.latimes.com/news/printedition/opinion /opinion/la-oe-boot20jul20,1,15721483.column (accessed July 20, 2005)

2. Jinn, Guo-Woei. "China's development of asymmetric warfare and the security of Taiwan and the Republic of China," Master's Thesis, Naval Postgraduate School (2004)

3. "China's defense policy" http:// www.fas.org/nuke/guide/china/doctrine/ (accessed August 8, 2005)

4. Jane's Document "China introduction." http://www4.janes.com/K2/doc.jsp?K2DocKey=/content1/janesdata/srep/srep081/s0810005.htm@current&QueryText=<AND>(<OR>(([80](china%20<AND>%20introduce)%20<IN>%20body),%20([100]([100](china%20<AND>%20introduce)%20<IN>%20title)%20<AND>%20([100](china%20<AND>%20introduce)%20<IN>%20body))))&Prod_Name=SREP081&image=browse&#Ref1 (accessed August 10, 2005)

5. Jane's Document "Intention to deceive: Iraqi misdirection of UN inspectors." http://www4.janes.com/K2/doc.jsp?t=Q&K2DocKey=/content1/janesdata/mags/jir/history/jir2004/jir00863.htm@current&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5DIraq+%3CIN%3E+body%29%2C+%28%5B100%5D%28%5B100%5DIraq+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5DIraq+%3CIN%3E+body%29%29%29%29&Prod_Name=JIR& (accessed August 18, 2005)

6. Patricia M. Fornes "Modernizing China's Air Force: Its strategy, budget, and capability." *Jane's Intelligence Review* (1995)

7. Vincent Wei-Cheng Wang and Gwendolyn Stamper "Asymmetric war? Implications for China's information warfare" *American Asian Review*(2002)

8. "From Canadian Bankruptcy to the Riches of Kazakhstan." *New York Times* (2005)

9. "Korean War" http://education.yahoo.com/reference/encyclopedia/entry/KoreanWa (accessed December 2005)

10. Don Kirk. “World Briefing Asia: South Korea: War Games With U.S.” *New York Times* (August 21, 2001).

11. The History Place “The Vietnam War.” http://www.historyplace.com/unitedstates/vietnam/index.html (accessed September 9, 2005)

12. Bradley Graham. “Hackers Attack Via Chinese Web Sites; U.S. Agencies’ Networks Are Among Targets.” *The Washington Post* (August 25, 2005)

13. Yoshihara, Toshi “Chinese Information Warfare: A Phantom Menace or Emerging Threat?” *University Press of the Pacific* (2004)

14. Potomac “New Technology Transfers to China on Hold, Pentagon Official Confirms” *Defense Daily International* (June 17, 2005).

15. Jane’s Document View “Jane’s Sentinel Security Assessment –China: Army.” http://www4.janes.com/K2/doc.jsp?K2DocKey=/content1/janesdata/sent/cnasu/chins110.htm@current&QueryText=<AND>(<OR>(([80]PLA%20<IN>%20body),%20([100]([100]PLA%20<IN>%20title)%20<AND>%20([100]PLA%20<IN>%20body))))&Prod_Name=CNAS&image=browse&#toclink-j0010002721 (accessed September 28, 2005).

16. Jane’s Document View “Jane’s Sentinel Security Assessment –China: Navy.” http://www4.janes.com/K2/doc.jsp?t=Q&K2DocKey=/content1/janesdata/sent/cnasu/chins130.htm@current&QueryText=%3CAND%3E%28%3COR%3E%28%28%5B80%5DPLA+%3CIN%3E+body%29%2C+%28%5B100%5D%28%5B100%5DPLA+%3CIN%3E+title%29+%3CAND%3E+%28%5B100%5DPLA+%3CIN%3E+body%29%29%29%29&Prod_Name=CNAS& (accessed September 28, 2005)

17. Jane’s Document View “Jane’s Sentinel Security Assessment –China: Air force.” Retrieved from the World Wide Web on September 28 2005 from http://www4.janes.com/K2/doc.jsp?K2DocKey=/content1/janesdata/sent/cnasu/chins120.htm@current&QueryText=<AND>(<OR>(([80](China%20<AND>%20Air%20<AND>%20Force)%20<IN>%20body),%20([100]([100](China%20<AND>%20Air%20<AND>%20Force)%20<IN>%20title)%20<AND>%20([100](China%20<AND>%20Air%20<AND>%20Force)%20<IN>%20body))))&Prod_Name=CNAS&image=browse&#toclink-j0010003722 (accessed September 28, 2005)

18. Jane's Document View "Jane's Sentinel Security Assessment – China: Second Artillery Corps." http://www4.janes.com.libproxy.nps.navy.mil/K2/doc.jsp?t=A&K2DocKey=/content1/janesdata/srep/srep085/s0850005.htm@current&QueryText=%3CAND%3E%28%3COR%3E%28PLA+%3CAND%3E+Second+%3CAND%3E+Artillery+%3CAND%3E+Corps+%29%29&Prod_Name=SREP085& (accessed September 28, 2005)

19. Lonnie Henley. "PLA LOGISTICS AND DOCTRINE REFORM." *Parameters* (2000)

20. Page E. Small. "China's Naval Modernization and Implications for the South China Sea." Master's Thesis, Naval Postgraduate School (December 2002)

21. "The PLA Navy and Active Defense." http://www.globalsecurity.org/military/ library/ report/2003/pla-china_transition_11_ch07.htm (accessed on September 30, 2005)

22. China's National Defense Report 2004

23. Swanson, Bruce. "China's Emerging Navy." *The China Business Review* (1984)

24. Horley "China plans progress while others look on." *Jane's Defense Weekly* (February 18, 1998)

25. Barbara W. Tuchman. "Stilwell and the American Experience in China 1911-1945." *The Macmillan company* (1970)

26. Shambaugh, David. "A Matter of Time: Taiwan's Eroding Military Advantage." *Washington Quarterly* (2000)

27. Shambaugh, David. 2004. *Modernizing China's Military: Progress, Problems, and Prospects.* Los Angeles, CA: University of California Press.

28. *Dumbaugh, Kerry*. "The Future of U.S.-China Relations by the Center for Strategic and International Studies" *The China Quarterly* (December 1993)

29. Kate Farris" Chinese view on information warfare" *Defense Intelligence Journal*(2001)

30. Norman Friedman. "How Will Chinese Military Modernize?" *United States Naval Institute* (September 2004).

31. Wade Boese.“United States Unsure of Chinese Military’s Modernization Aims.” *Arms Control Today* (September 2005).

32. “Pentagon’s ‘China Report’ Warns of Consequences of Lifting EU Arms Embargo.” *Potomac* (July 29, 2005).

33. Chris Buckley. **“**China and European Union Discuss Trade Ties and Arms Embargo.” *New York Times* (May 12, 2005).

34. Frank Tiboni “The new Trojan War.” *Federal Computer Week* (August 22, 2005)

35. Eugene Schultz. “Information warfare between China and the US.” *Computers & Security* (2002)

36. Timothy L. Thomas. **“**China's electronic strategies.” *Military Review* (May/Jun 2001).

37. Timothy L .Thomas “Like Adding Wings to a Tiger: Chinese INFORMATION WAR THEORY AND PRACTICE” *Military Intelligence Professional Bulletin.* (July-September 2003).

38. Bradley K. Ashley. “The United States Is Vulnerable to Cyberterrorism.” *Signal* 58 (March 2004).

39. Timothy Hildebrandt. “Uneasy Allies: Fifty Years of China-North Korea Relations.” *Asia program special report* (September 2003)

40. Michael Hirsh, Melinda Liu. “North Korea Hold ’Em: Washington used to have most of the chips in six-party talks over Pyongyang’s nuclear program. But Beijing is the key player now--for better and worse.” *Newsweek* 146:14 (October 3, 2005), 42

41. Zhang, Xiaoming. “The Vietnam War, 1964-1969: A Chinese Perspective.” *The Journal of Military History* 60:4 (October 1996), 731

42. Robert G. Kaiser and Steven Mufson “Taiwan: Crisis in the Making? Experts Differ on Whether Rising Tensions Will Lead to a U.S.-China Clash.” *The Washington Post* (March 16, 2000), A.22

43. George Yeo. About Face: The U.S. ROLE IN THE ASIAN DREAM: America must stay engaged with the region even as China grows.” *Asiaweek* (April 20, 2001), 1 (cover story).

44. Timothy L Thomas. **“**Human network attacks.**”** *Military Review* 79:5 (September/October 1999), 23.

45. "Electronic Warfare. http://usmilitary.about.com/library/glossary/e/bldef02162.htm ?iam=metaresults&terms=electronics (accessed October 19, 2005).

46. Kernan Chaisson. **"**A direct approach to SEAD and attacks on C2." *Journal of Electronic Defense* 22:7 (July 1999), 16

47. Kernan Chaisson. **"**EW big winner in Kosovo.**"** *Journal of Electronic Defense* 22:12 (December 1999), 15

48. **"**China: Information Warfare.**"** *OxResearch* (April 20, 1999), 1

49. Peter C. Newman. **"**World hackers unite!**"** *Maclean's* 114:35 (August 27, 2001), 14

50. Nathan Vardi. "Chinese Take Out." *Forbes* 176:2 (July 25, 2005), 54

51. B. Rivers "Israel supplying China with AEW system" *Journal of Electronic Defense* 22:12 (December 1999), 22

52. Robert Wall. "Chinese Advance in Electronic Attack." *Aviation Week & Space Technology* 157:18 (October 28, 2002), 70

53. James Adams. "Virtual Defense." *Foreign Affairs* 80:3 (May/June 2001).

54. Arreguin Toft. "How the Weak Win the Wars." *Cambridge University Press* (December 2005)

55. Damon Bristow "Information warfare grips China" *Jane's Intelligence Review* (November 1, 1998)

56. Ezio Bonsignore and Eugene Kogan "Fatal Attraction: The EU Defence Industry and China." *Military Technology* 29:6 (June 2005), 8

57. Elisabeth Bumiller. "Bush Says Europe Should Not Lift China Arms Ban." *New York Times* (February 23, 2005), A1

58. "Urging the European Union to maintain its arms export embargo on the People's Republic of China." http://fas.org/asmp/resources/govern/109th/sres91.htm (accessed October 28, 2005)

59. Zalmay Khalilzad, ed., *Strategic Appraisal 1996*(Santa Monica, Ca.: Rand, 1996), 215

60. June Teufel Dreyer. "Mixed Motives, Uncertain Outcomes: Defense Conversion in China/The Complete Art of War." *Pacific Affairs* 71:3 (fall 1998), 413

61. "China angry at Google map change." http://news.bbc.co.uk/w/hi/asiapacific/ 4356276.stm (accessed October 31, 2005)

62. Amy Svitak. "Digital China a potent potential foe: Nation first to information-warfare." *Time. New York* (December 23, 2002)

63. Jane's Document View "Information Technology" *China's Aerospace And Defense Industry* (December 2000)

64. Bennis Wai Yip So "The New Knowledge Economy of Taiwan" *The China Journal* (Canberra) 53 (January 2005), 174

65. Kyna Rubin. *"China's Students Turning Away or Staying Home." International Educator* (summer 2004)

66. "U.S. charges 4 China spy suspects." http://edition.cnn.com/2005/LAW/11/05/ navy.indictments.ap/index.html (accessed November 5, 2005)

67. PAUL RICHTER. "Ancient Doctrine Guiding Futuristic Warfare in Gulf Strategy: Sun Tzu's tiny book, written more than 2,500 years ago, is influencing U.S. and Iraqi tactics." *Los Angeles Times* (February 18, 1991), A1

68. DAN SEWELL. "The Art of War: Learning How to Fight, According to the Book of Books: "The Art of War" by Sun Tzu contains a Chinese militarist's centuries-old advice that still rings true for personal and global conflicts." *Los Angeles Times* (November 23, 1989), 20

69. Tim Thomas. "China's technology stratagems." *Jane's Intelligence Review* (December 2000)

70. Timothy L Thomas. "Confrontation central to Chinese IW aims." *Jane's Intelligence Review* (June 2002)

71. "The Trojan War." http://www.stanford.edu/~plomio/history.html (accessed November 14, 2005)

72. "Muhammad Ali Biographical Sketch." http://www.ali.com/article.cfm?id=26 (accessed November 9, 2005)

73. Andrew J.R. Mack. "Why Big Nations Lose Small Wars." *World Politics* (1975)

74. "About Lenovo." http://www.lenovo.com/lenovo/us/en/ (accessed November 19, 2005)

75. "China's design on US energy." *Jane's Information Group* (August 18, 2005)

76. "Lenovo's IBM Acquisition Tests U.S. China Policy." http://www.defensenews.com/story.php?F=723266&C=commentary (accessed July 3, 2005)

77. "Lenovo releases China's first security chip." http://www.english.people.com.cn/ 200504/12/eng20050412_180617.html (accessed November 19, 2005)

78. Frederick W. Stakelbeck Jr. "The Approach Chinese Cyber Storm." *FrontPageMagazine.com* (July 21, 2005)

79. "China's policy of sending students abroad remains unchanged." *The Xinhua General Overseas New Service* (April 5, 1998)

80. "The PLA also used Chinese students trained at American universities." *The Washington Times* (November 1999)

81. "Science and Engineering Indicators 2004." http://www.nsf.gov/statistics/seindo4/ c2/c2s4.htm (accessed November 30, 2005)

82. "Boeing, IBM join hands on military information technology." http://english.people .com.cn/ (accessed November 19, 2005)

83. "The US/China Cyber war of April/May 2001." http://www.happyhacker.org/news/ china.shtml (accessed January 6, 2006)

84. Nathan Thornburgh. "The Invasion of Chinese Cyberspies (And the Man Who Tried to Stop Them)." *Time. New York* (September 5, 2005)

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Prof. Karl D. Pfeiffer
   Naval Postgraduate School
   Monterey, California

4. Glen Cook
   Naval Postgraduate School
   Monterey, California

5. CPT. Tsai Wen-Hsiang
   Naval Postgraduate School
   Monterey, California

6. Dan C. Boger
   Naval Postgraduate School
   Monterey, California